

DATA TRANSFERRING SYSTEM, DATA TRANSFERRING DEVICE, DATA RECORDING DEVICE, DATA MANAGING METHOD AND IDENTIFIER GENERATING METHOD

Publication number: JP2002366441 (A)

Publication date: 2002-12-20

Inventor(s): ABE MIKI; HOSOI TAKASHI; MATSUDA HIROMI; TANAKA YOSHIO

Applicant(s): SONY CORP

Classification:

- international: G06F12/14; G06F12/00; G06F21/00; G06F21/24; G09C1/00; G11B20/00; G11B27/034; G11B27/10; H04L9/08; H04L29/06; H04N7/173; G11B20/10; G11B20/12; G06F12/14; G06F12/00; G06F21/00; G09C1/00; G11B20/00; G11B27/031; G11B27/10; H04L9/08; H04L29/06; H04N7/173; G11B20/10; G11B20/12; (IPC1-7): G06F12/14; G06F12/00; G09C1/00; H04L9/08; H04N7/173

- European: H04L29/06S4B; G06F21/00N7D; G11B20/00P; G11B27/034; G11B27/10A1

Application number: JP20010178512 20010613

Priority number(s): JP20010178512 20010613

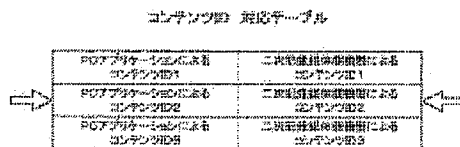
Also published as:

JP3778009 (B2)
US2004015713 (A1)
US7350238 (B2)
RU2284591 (C2)
WO02103529 (A1)

more >>

Abstract of JP 2002366441 (A)

PROBLEM TO BE SOLVED: To realize the proper management and operating efficiency of contents transfer. **SOLUTION:** A data transferring device side (primary recording medium side) manages the transfer right of respective stored contents data, and also manages the transfer right of contents data transferred to a data recording device (secondary recording medium side) in a state that table data in which a first contents identifier corresponding to the contents data is made correspond to a second contents identifier transmitted from the recording device side are generated.; That is, even when it is not possible to record the contents identifier (contents ID) at the secondary recording medium side, it is possible to identify the contents data on the secondary recording medium by using the contents ID (second contents identifier) generated at the secondary recording medium side, and to make this correspond to the contents ID (first contents identifier) at the primary recording medium side.



Data supplied from the esp@cenet database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-366441

(P2002-366441A)

(43) 公開日 平成14年12月20日 (2002. 12. 20)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
12/00	5 3 7	12/00	5 3 7 H 5 B 0 8 2
	5 4 5		5 4 5 M 5 C 0 6 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 J 1 0 4
H 0 4 L 9/08		H 0 4 N 7/173	6 3 0

審査請求 未請求 請求項の数25 O L (全 49 頁) 最終頁に続く

(21) 出願番号 特願2001-178512(P2001-178512)

(22) 出願日 平成13年6月13日(2001. 6. 13)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 阿部 三樹

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 細井 隆史

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100086841

弁理士 脇 篤夫 (外1名)

最終頁に続く

(54) 【発明の名称】 データ転送システム、データ転送装置、データ記録装置、データ管理方法、識別子生成方法

(57) 【要約】

【課題】 コンテンツ転送の適切な管理及び動作の効率化。

【解決手段】 データ転送装置側（一次記録媒体側）では、格納されている各コンテンツデータについての転送権利を管理するとともに、データ記録装置（二次記録媒体側）に対して転送したコンテンツデータについては、そのコンテンツデータに対応する第1のコンテンツ識別子とデータ記録装置側から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する。つまり二次記録媒体側でコンテンツ識別子（コンテンツID）を記録できない場合でも、二次記録媒体側で発生させるコンテンツID（第2のコンテンツ識別子）を用いて二次記録媒体上のコンテンツデータを識別でき、しかもそれが一次記録媒体側のコンテンツID（第1のコンテンツ識別子）と対応づけられるようにする。

コンテンツID 対応テーブル

PCアプリケーションによる コンテンツID1	二次記録媒体側機器による コンテンツID1
PCアプリケーションによる コンテンツID2	二次記録媒体側機器による コンテンツID2
PCアプリケーションによる コンテンツID3	二次記録媒体側機器による コンテンツID3

【特許請求の範囲】

【請求項1】 データ転送装置と、データ記録装置とから成るデータ転送システムにおいて、
 上記データ転送装置は、
 一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、
 暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第1のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、
 上記データ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、
 上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して転送したコンテンツデータについては、該コンテンツデータに対応する上記第1のコンテンツ識別子と上記データ記録装置側から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、
 を備え、
 上記データ記録装置は、
 上記データ転送装置との間で、コンテンツデータの受信を含む各種データ通信を行う通信手段と
 二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、
 上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態に復号する復号手段と、
 上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、
 非暗号化状態のコンテンツデータから上記第2のコンテンツ識別子を生成する識別子生成手段と、
 上記識別子生成手段で生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、
 を備えたことを特徴とするデータ転送システム。

【請求項2】 上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理することを特徴とする請求項1に記載のデータ転送システム。

【請求項3】 上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第2のコンテンツ識別子を要求し、送信されてきた第2のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項1に記載のデータ転送システム。

【請求項4】 上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイン

トによりコンテンツデータの一部分を抽出し、抽出したデータを用いた演算処理により上記第2のコンテンツ識別子を生成することを特徴とする請求項1に記載のデータ転送システム。

【請求項5】 上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた1又は複数のポイントとされることを特徴とする請求項4に記載のデータ転送システム。

【請求項6】 上記データ転送装置からコンテンツデータが転送されてくる際に、
 上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記第2のコンテンツ識別子を生成し、
 上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項4に記載のデータ転送システム。

【請求項7】 コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合に、
 上記二次記録媒体ドライブ手段は、
 上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、
 上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第2のコンテンツ識別子が要求された際には、
 上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記第2のコンテンツ識別子を生成し、
 上記識別子送信制御手段は、生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項4に記載のデータ転送システム。

【請求項8】 コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合に、
 上記二次記録媒体ドライブ手段は、
 上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、
 上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記第2のコンテンツ識別子を生成して記憶手段に記憶させておき、
 上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第2のコンテンツ識別子が要求された際には、
 上記識別子送信制御手段は、上記記憶手段に記憶されて

いる上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項4に記載のデータ転送システム。

【請求項9】 一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第1のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、外部のデータ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して或るコンテンツデータを転送した際には、該コンテンツデータに対応する上記第1のコンテンツ識別子と上記データ記録装置側から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、を備えたことを特徴とするデータ転送装置。

【請求項10】 上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理することを特徴とする請求項9に記載のデータ転送装置。

【請求項11】 上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第2のコンテンツ識別子を要求し、送信されてきた第2のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項9に記載のデータ転送装置。

【請求項12】 外部のデータ転送装置との間で、コンテンツデータの受信を含む各種データ通信を行う通信手段と二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態に復号する復号手段と、上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、非暗号化状態のコンテンツデータからコンテンツ識別子を生成する識別子生成手段と、上記識別子生成手段で生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、を備えたことを特徴とするデータ記録装置。

【請求項13】 上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理により上記コンテンツ識別子を

生成することを特徴とする請求項12に記載のデータ記録装置。

【請求項14】 上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた1又は複数のポイントとされることを特徴とする請求項13に記載のデータ記録装置。

【請求項15】 上記データ転送装置からコンテンツデータが転送されてくる際に、上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記コンテンツ識別子を生成し、上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項13に記載のデータ記録装置。

【請求項16】 コンテンツデータが記録された上記二次記録媒体が装填されている場合に、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記コンテンツ識別子が要求された際には、上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記コンテンツ識別子を生成し、上記識別子送信制御手段は、生成された上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項13に記載のデータ記録装置。

【請求項17】 コンテンツデータが記録された上記二次記録媒体が装填されている場合に、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記コンテンツ識別子を生成して記憶手段に記憶させておき、上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記コンテンツ識別子が要求された際には、上記識別子送信制御手段は、上記記憶手段に記憶されている上記コンテンツ識別子を上記通信手段により上記データ転送装置に送信させることを特徴とする請求項13

に記載のデータ記録装置。

【請求項18】 暗号化されて一次記録媒体に記録されたコンテンツデータについての、二次記録媒体への転送権利を管理するデータ管理方法において、
上記各コンテンツデータについて生成した第1のコンテンツ識別子にそれぞれ対応させて、各コンテンツデータの転送権利を管理すると共に、
二次記録媒体へ転送したコンテンツデータについては、
該コンテンツデータに対応する上記第1のコンテンツ識別子と上記二次記録媒体側機器から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理することを特徴とするデータ管理方法。

【請求項19】 各コンテンツデータについての上記転送権利として、外部の二次記録媒体に対する転送許可回数を管理することを特徴とする請求項18に記載のデータ管理方法。

【請求項20】 二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、二次記録媒体側機器に対して、当該コンテンツデータについての上記第2のコンテンツ識別子を要求し、送信されてきた第2のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新することを特徴とする請求項18に記載のデータ管理方法。

【請求項21】 コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理によりコンテンツ識別子を生成することを特徴とする識別子生成方法。

【請求項22】 上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた1又は複数のポイントとされることを特徴とする請求項21に記載の識別子生成方法。

【請求項23】 暗号化されたコンテンツデータが受信され、非暗号化状態で復号されて記録媒体に記録される場合に、
復号されたコンテンツデータが上記記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理によりコンテンツ識別子を生成することを特徴とする請求項21に記載の識別子生成方法。

【請求項24】 記録媒体に記録されている各コンテンツデータについて、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生して記憶しておき、
上記外部機器から上記記録媒体に記録されているコンテンツデータについてのコンテンツ識別子が要求された際に、上記記憶したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成することを特

徴とする請求項21に記載の識別子生成方法。

【請求項25】 記録媒体に記録されている各コンテンツデータについて、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生し、再生したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成して記憶しておくことを特徴とする請求項21に記載の識別子生成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、音楽等のコンテンツデータの転送／記録に好適な、データ転送システム、データ転送装置、データ記録装置、データ管理方法、識別子生成方法に関するものである。

【0002】

【従来の技術】例えばパーソナルコンピュータのHDD（ハードディスクドライブ）を一次記録媒体として扱って音楽等のコンテンツデータを格納するとともに、格納したコンテンツデータを転送して他の記録媒体（二次記録媒体）に記録し、その二次記録媒体側で音楽等の再生を楽しむという使用形態がある。なおコンテンツデータとは、例えば音楽データ、映像データ、ゲームデータ、コンピュータソフトウェアなどの配信／転送／使用の目的となる主たるデータのことである。

【0003】この場合、HDDには、CD-DA（Compact Disc Digital Audio）やDVD（Digital Versatile Disc）などのパッケージメディアから再生された音楽等のコンテンツデータが蓄積されたり、或いはパーソナルコンピュータが接続された通信ネットワークを介して外部の音楽サーバ等からダウンロードされたコンテンツデータが蓄積される。そしてユーザーは、パーソナルコンピュータに二次記録媒体の記録装置を接続して、HDDに蓄積されたコンテンツデータを二次記録媒体にコピー（複製）又はムーブ（移動）し、当該二次記録媒体に対応する再生装置で音楽等のコンテンツデータを再生させる。

【0004】二次記録媒体としては、例えばフラッシュメモリ等の半導体メモリを利用したメモリカードや、光磁気ディスクとしてのミニディスク、或いはCD-R（CD Recordable）、CD-RW（CD Rewritable）、DVD-RAM、DVD-R、DVD-RWなどが考えられる。二次記録媒体に対応する記録装置、再生装置として、これらのメディア（記録媒体）に対応するレコーダ／プレーヤーは、広く普及しており、据置型の記録再生装置や、ポータブルタイプの記録再生装置などとして多様に存在し、各ユーザーはそれぞれ自分の好みや所有する機器に合わせて、コンテンツデータの記録／再生を行うものとなる。

【0005】なお、例えばこのようなコンテンツデータの使用形態を考えると、コンテンツデータについて

の著作権保護を考慮しなければならない。例えばユーザーがコンテンツデータの配信サービスを利用したり、パッケージメディアの購入を行うなどして、HDDにコンテンツデータを蓄積した後、そのコンテンツデータを無制限に二次記録媒体にコピー可能とすると、著作権者の正当な保護がはかれない事態が生ずる。このためデジタルデータとしてのコンテンツデータの扱い上で著作権保護を維持できるようにする様々な技術やデータ処理上の取り決めが提案されているが、その1つにSDMI (SECURE DIGITAL MUSIC INITIATIVE) という規格がある。このSDMIで策定されたデータパスについては後述するが、例えば一次記録媒体としてのHDDを備えたパーソナルコンピュータに蓄積されたコンテンツ、例えばネットワークを介して外部サーバから配信されたコンテンツデータ（以下、ネットワークコンテンツ）や、例えばパーソナルコンピュータに装備されているCD-ROMドライブ等のディスクドライブ装置、或いはパーソナルコンピュータと接続されたディスクドライブ装置において再生されるCD-DA、DVD等のパッケージメディアから読み出されたコンテンツデータ（以下、ディスクコンテンツ）について、二次記録媒体への転送／記録が、著作権保護と一般ユーザーの利益（私的複製の権利）を勘案したうえで、適切に行われるようにされている。

【0006】ところで、HDD等の一次記録媒体からミニディスクやメモ리카ード等の二次記録媒体へコンテンツデータを転送してコピーする場合においては、上記のように著作権保護や私的複製の権利の双方を満たすための工夫が施されている。

【0007】即ち上記SDMI対応の二次記録媒体に対する転送については次のようになっている。SDMI対応の二次記録媒体とは、例えばフラッシュメモリ等の半導体メモリを利用したSDMI対応のメモ리카ードなどが想定され、この二次記録媒体にはコンテンツが暗号化された状態で記録される。例えばHDDなどの一次記録媒体では、SDMI方式のコンテンツの場合は暗号化が施されて蓄積されるが、従って、その暗号化状態のまま二次記録媒体にコピーされるものとなる。もちろん二次記録媒体に対する再生機器では、暗号解読機能が備えられており、従って暗号化状態でコピーされたコンテンツデータを再生させることができる。

【0008】またSDMI対応の二次記録媒体では各コンテンツデータについての識別子となるコンテンツIDを記録する領域がフォーマット上、用意されている。コンテンツIDは、一次記録媒体側の機器において一次記録媒体（HDD）に蓄積された各コンテンツデータについて生成し、コンテンツデータとともに格納しておくものであるが、コンテンツデータを二次記録媒体にコピーする場合には、そのコンテンツデータについてのコンテンツIDも、二次記録媒体に記録されるものとなる。

【0009】コンテンツIDは、一次記録媒体側と二次記録媒体側でのコンテンツ権利管理に用いられる。ここでいうコンテンツ権利とは、一次記録媒体側については、二次記録媒体への転送権（二次記録媒体にコピーさせる権利）であり、二次記録媒体側については、コピーしたコンテンツデータの再生権となる。なお、以下、一次記録媒体から二次記録媒体へのコンテンツデータの転送（権利譲渡）を「チェックアウト」といい、また二次記録媒体から一次記録媒体へのコンテンツデータの返却（実際には権利の返却）を「チェックイン」と呼ぶ。

【0010】SDMI方式では、チェックアウト、チェックインに関しては、転送の取り扱いルール（Usage Rule）が決められる。一例としては、1つのコンテンツデータについて、一次記録媒体から二次記録媒体へのチェックアウトは3回許される（上記転送権は「3回」となる）。チェックアウトが行われると、権利が二次記録媒体側へ譲渡されることになり、つまり一次記録媒体側では、そのコンテンツデータの転送権の残りは2回となる。一方、二次記録媒体側では再生権を得ることになる。また、二次記録媒体から一次記録媒体にチェックインを行うと、権利が返却されるものとなる。つまり、二次記録媒体側では再生権を失い、一次記録媒体側では転送権が1つ復活される。

【0011】このようなチェックアウト／チェックインの管理は、各コンテンツデータ毎にコンテンツIDを用いて行われる。そしてチェックアウトの際には、コンテンツデータ及びコンテンツIDが二次記録媒体側に記録されることで、二次記録媒体側ではコンテンツデータの再生が可能となる（再生権を得る）。一次記録媒体では、コンテンツIDを1つ譲渡したとみなして、Usage Ruleによる転送権を1つ減少させる。またチェックインの際には、実際にはコンテンツデータの返却転送は行われず、二次記録媒体でコンテンツデータを消去し、一次記録媒体側ではコンテンツIDが返却されたとして、Usage Ruleによる転送権を1つ増加させる。二次記録媒体側では再生権を失うことになる。

【0012】このようにSDMI対応の二次記録媒体については、コンテンツデータが暗号化状態でコピー記録されること、及びチェックアウト、チェックインに応じてコンテンツの権利が管理されることで、無制限なコピーを防止して著作権保護をはかり、又一方でユーザーの私的複製権を確保している。

【0013】なお、例えば外部サーバから一次記録媒体としてのHDDにダウンロードされて格納されるコンテンツデータは、コンテンツキーCKで暗号化されたものである。本明細書における説明上、一次記録媒体であるHDDには、ATRAC3方式（もちろん他の圧縮方式でもよいが）で圧縮されたコンテンツデータ「A3D」がコンテンツキーCKで暗号化されて格納されているとする。

【0014】そして、本明細書では説明上、鍵（キー） x で暗号化されたデータ y を、

$E(x, y)$

と表す。またその暗号化データ $E(x, y)$ について、鍵 x により暗号化を復号したデータを、

$D\{x, E(x, y)\}$

と表すこととする。従って、例えば上記のようにATRAC3方式の圧縮データを「A3D」とすると、コンテンツキーCKで暗号化されたコンテンツデータ「A3D」は、

$E(CK, A3D)$

となる。また $E(CK, A3D)$ が、鍵CKで復号されたデータは、

$D\{CK, E(CK, A3D)\}$

と表わせられる。

【0015】また一次記録媒体であるHDDには、暗号化コンテンツデータ $E(CK, A3D)$ とともに、ルートキーKRで暗号化された状態のコンテンツキーCK、つまり、 $E(KR, CK)$ も格納される。例えば外部サーバから暗号化コンテンツデータ $E(CK, A3D)$ とともに、暗号化コンテンツキー $E(KR, CK)$ がダウンロードされる。この場合、一次記録媒体であるHDDから二次記録媒体にコンテンツデータを転送する場合、暗号化コンテンツデータ $E(CK, A3D)$ と暗号化コンテンツキー $E(KR, CK)$ を送信すればよい。二次記録媒体側機器では、ルートキーKRを保持していることで、ルートキーKRを用いてコンテンツキーCKを復号し、さらに復号したコンテンツキーCKを用いて暗号化コンテンツデータを復号できるものとなる。ただしルートキーKRは、著作権者側の意志や各種事情によって変更されるものであり、コンテンツデータ毎に異なるルートキーKRを設定することもできる。また具体例については後述するが、ルートキーKRの処理によってコンテンツ配信先を限定できる機能を有する。このため、EKB（Enabling Key Block：有効化キープブロック）と呼ばれるデータが配信されることもあり、コンテンツデータが転送される正規の端末では、EKBによってルートキーを確認できるようにした方式も採られている。つまりEKBも上記暗号化コンテンツデータや暗号化コンテンツキーとともにサーバから配信されてHDDに格納される。

【0016】

【発明が解決しようとする課題】ここで、現在広く普及しているミニディスク（光磁気ディスク）を二次記録媒体として用いることを考える。例えばSDMI対応のミニディスク記録装置を考える場合、そのミニディスク記録装置は、チェックアウトされたコンテンツデータについて、暗号化されたままの $E(CK, A3D)$ の状態でもミニディスクに記録するものとされる。そして再生時にはSDMI対応のミニディスク再生装置が、 $D\{CK,$

$E(CK, A3D)\} = A3D$ として暗号解読されたATRAC3データ（A3D）を得たうえで、所定のデコード処理を行って音楽等の再生出力を行うことになる。

【0017】一方、一般に普及しているミニディスクシステムでは、ミニディスクに暗号化データを記録するものではない。当然、ミニディスク再生装置としては暗号解読の機能はない。従って、SDMI対応のミニディスク記録装置でコンテンツデータをミニディスクに記録したとしても、そのミニディスクに記録されたコンテンツデータを、SDMI対応でない多くのミニディスクプレーヤーでは再生できないものとなる。つまり再生互換性が得られない。これは、一般ユーザーが購入したSDMIコンテンツの適正な利用を制限するものとなり、一般ユーザーに対するSDMIコンテンツ提供サービスの価値や満足度を大きく低下させることがある。

【0018】このような点を考慮すると、SDMIコンテンツを二次記録媒体にコピー記録する際に、暗号化を解いた状態で、例えばSDMIに対応していないミニディスク記録装置に転送し、そのまま暗号化されていない状態でミニディスク等の二次記録媒体に記録できるようにすることが考えられる。しかしながらそのようなコピーを可能とすることは、コンテンツデータのコピーを容易に可能とすることになる。これは違法なコピーが可能となる余地を残してしまうことにもなり、SDMIの本来の目的である著作権保護が実現できないおそれがある。

【0019】そこでコンテンツデータ転送の一手法として、次のような転送方式を本出願人は先に提案している。即ち、コンテンツデータ転送の際には、データ転送装置（一次記録媒体側機器）が転送先となるデータ記録装置（二次記録媒体側機器）の認証を行い、認証OKとなること、及びコンテンツ提供者側（著作権者等）の許諾があることを条件としてコンテンツデータを転送許可する。そしてコンテンツデータは暗号化状態で伝送路上を転送するが、二次記録媒体へは暗号化を解いて記録するものである。また、チェックアウト、チェックインについての権利管理も行われる。これによって、非暗号化状態でのコピー記録を許容してユーザーの便宜を図ると共に、著作権保護機能が失われないようにする。

【0020】しかしながらこのような転送方式については、以下のような問題がある。従来より普及しているミニディスク等のメディアを二次記録媒体として、SDMIコンテンツのチェックアウト／チェックインを行おうとする場合、ミニディスク側にコンテンツIDを記録できないという事情がある。つまりミニディスク上ではコンテンツIDを記録する領域は用意されていないし、また既に普及しているミニディスクレコーダではコンテンツIDを管理する機能がない。例えばミニディスクの管理領域（U-TOC）などにコンテンツIDを記録する領域を新たに設定することはできても、従前のミニディ

スクレコードで記録や編集が行われてU-TOCが更新されてしまえば、コンテンツIDは失われてしまう。つまり従前の機器との互換性を得てユーザーの便宜を図ることで、ミニディスク側でコンテンツIDを管理できない。そしてコンテンツIDが管理できないため、例えばチェックイン管理ができないものとなる。

【0021】一方、ミニディスク等の二次記録媒体側で例えばコンテンツデータそのものから各コンテンツデータの識別子となるコンテンツIDを生成することは可能である。しかしながらコンテンツIDの生成のためにはディスクをシークしてコンテンツデータの一部の読出などが必要であり、処理に時間がかかるという難点があると共に、そのようにして二次記録媒体側でコンテンツIDを生成しても、一次記録媒体側のコンテンツIDと一致しないため、結局管理不能となる。

【0022】

【課題を解決するための手段】本発明はこのような事情に依拠して、一次記録媒体と、非暗号化状態でコンテンツデータを記録する二次記録媒体との間でのコンテンツデータの転送管理を適切に行うことができるようにし、また処理の効率化を実現することを目的とする。

【0023】このため本発明では、データ転送装置と、データ記録装置とから成るデータ転送システムを提供する

【0024】そして本発明のデータ転送装置は、一次記録媒体に対してデータの記録再生を行う一次記録媒体ドライブ手段と、暗号化されたコンテンツデータ及び該コンテンツデータに固有に生成した第1のコンテンツ識別子を、上記一次記録媒体に格納させる格納制御手段と、上記データ記録装置との間で、コンテンツデータの転送を含む各種データ通信を行う通信手段と、上記各コンテンツデータについての転送権利を管理するとともに、上記データ記録装置に対して転送したコンテンツデータについては、該コンテンツデータに対応する上記第1のコンテンツ識別子と上記データ記録装置側から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する転送管理手段と、を備えるものとする。

【0025】また、上記転送管理手段は、各コンテンツデータについての上記転送権利として、外部のデータ記録装置に対する転送許可回数を管理する。また上記転送管理手段は、上記二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際に、上記データ記録装置に対して、当該コンテンツデータについての上記第2のコンテンツ識別子を要求し、送信されてきた第2のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新する。

【0026】また本発明のデータ記録装置は、上記データ転送装置との間で、コンテンツデータの受信を含む各

種データ通信を行う通信手段と二次記録媒体に対してデータの記録再生を行う二次記録媒体ドライブ手段と、上記データ転送装置から送信されてくる暗号化されたコンテンツデータを非暗号化状態で復号する復号手段と、上記復号手段で復号されたコンテンツデータを上記二次記録媒体ドライブ手段により上記二次記録媒体に記録させる記録制御手段と、非暗号化状態のコンテンツデータから上記第2のコンテンツ識別子を生成する識別子生成手段と、上記識別子生成手段で生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる識別子送信制御手段と、を備えるようにする。

【0027】また上記識別子生成手段は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理により上記第2のコンテンツ識別子を生成する。この場合、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた1又は複数のポイントとする。

【0028】また、上記データ転送装置からコンテンツデータが転送されてくる際に、上記識別子生成手段は、上記復号手段で復号されたコンテンツデータが上記二次記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により上記第2のコンテンツ識別子を生成し、上記識別子送信制御手段は、上記データ転送装置からのコンテンツデータ転送完了後に、上記識別子生成手段で生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合には、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶手段に記憶させておき、上記データ転送装置から上記二次記録媒体に記録されているコンテンツデータについての上記第2のコンテンツ識別子が要求された際には、上記識別子生成手段は、上記記憶手段に記憶されたサンプリングポイントのデータを用いた演算処理により上記第2のコンテンツ識別子を生成し、上記識別子送信制御手段は、生成された上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。又は、コンテンツデータが記録された上記二次記録媒体がデータ記録装置に装填されている場合には、上記二次記録媒体ドライブ手段は、上記二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生し、上記識別子生成手段は、上記再生されたサンプリングポイントのデータを用いた演算処理により上記各コンテンツデータについての上記第2のコンテンツ識別子を生成して記憶手段に記憶させておき、上記データ転送装

置から上記二次記録媒体に記録されているコンテンツデータについての上記第2のコンテンツ識別子が要求された際には、上記識別子送信制御手段は、上記記憶手段に記憶されている上記第2のコンテンツ識別子を上記通信手段により上記データ転送装置に送信させる。

【0029】本発明のデータ管理方法は、暗号化されて一次記録媒体に記録されたコンテンツデータについての、二次記録媒体への転送権利を管理するデータ管理方法として、上記各コンテンツデータについて生成した第1のコンテンツ識別子にそれぞれ対応させて、各コンテンツデータの転送権利を管理すると共に、二次記録媒体へ転送したコンテンツデータについては、該コンテンツデータに対応する上記第1のコンテンツ識別子と上記二次記録媒体側機器から送信されてきた第2のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理する。この場合、各コンテンツデータについての上記転送権利として、外部の二次記録媒体に対する転送許可回数を管理する。また二次記録媒体に記録させた或るコンテンツデータについて、上記二次記録媒体側での再生権利を消失させる際には、二次記録媒体側機器に対して、当該コンテンツデータについての上記第2のコンテンツ識別子を要求し、送信されてきた第2のコンテンツ識別子を上記テーブルデータで照合した上で、該当するコンテンツデータについての転送権利を更新する。

【0030】本発明の識別子生成方法は、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツデータの一部を抽出し、抽出したデータを用いた演算処理によりコンテンツ識別子を生成する。この場合、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた1又は複数のポイントとする。また暗号化されたコンテンツデータが受信され、非暗号化状態に復号されて記録媒体に記録される場合に、復号されたコンテンツデータが上記記録媒体に記録されるまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理によりコンテンツ識別子を生成する。また記録媒体に記録されている各コンテンツデータについては、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生して記憶しておき、上記外部機器から上記記録媒体に記録されているコンテンツデータについてのコンテンツ識別子が要求された際に、上記記憶したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成する。或いは、記録媒体に記録されている各コンテンツデータについては、外部機器からのコンテンツ識別子の要求に先だって、予め上記サンプリングポイントのデータを記録媒体から再生し、再生したサンプリングポイントのデータを用いた演算処理によりコンテンツ識別子を生成して記憶しておく。

【0031】以上のような本発明によれば、データ転送装置とデータ記録装置との間のコンテンツデータのチェックアウト／チェックインに応じた権利管理を、第1、第2のコンテンツ識別子（コンテンツID）を用いて適正に行うことができる。またデータ記録装置側での第2のコンテンツ識別子の生成も効率化される。

【0032】

【発明の実施の形態】以下、本発明の実施の形態を次の順序で説明する。

1. 暗号化キーのツリー構造及びEKB
2. システム構成
3. SDMIコンテンツのデータパス
4. データ転送装置の構成例（一次記録媒体側機器／PC）
5. データ記録装置の構成例（二次記録媒体側機器／記録再生装置）
6. ミニディスクの管理方式
7. 認証処理
8. コンテンツ暗号化方式
9. 各種コマンド
10. コンテンツのチェックアウト／チェックイン
11. コンテンツIDの生成及び管理方式
12. チェックアウト時及びチェックイン前のコンテンツIDの生成処理
13. コンテンツ書込制御フラグ
14. 課金情報処理

【0033】1. 暗号化キーのツリー構造及びEKB
まず実施の形態の転送システムの具体的な説明に先立って、コンテンツ配信に用いられる暗号化方式キーの構造を説明する。このため図1、図2、図3を用いて、コンテンツ配信側からコンテンツ受信側の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵（キー）の保有構成およびデータ配信構成を説明していく。

【0034】図1は、暗号化キーのツリー構造を示しており、図1の最下段に示すナンバDV0～DV15がコンテンツ受信側となる個々のデバイスである。すなわち図示する階層ツリー構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

【0035】各デバイスDV0～DV15は、製造時あるいは出荷時、あるいはその後において、図1に示す階層ツリー構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。このキーセットはDNK（Device Node Key）と呼ばれるが、その具体例については後に説明する。図1の最下段に示すK0000～K1111が各デバイスDV0～DV15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）に続いて、最下段から2番目の節（ノード）に記載されたキー：K0～K

111をノードキーとする。なお文言上「ルートキー」も「ノードキー」に含むことがある。

【0036】図1に示すツリー構成において、例えばデバイスDV0は上記DNKとして、リーフキーK0000と、ノードキー：K000、K00、K0、ルートキーKRを所有する。例えばDNKにおいてはノードキー：K000、K00、K0、ルートキーKRをリーフキーK0000によって暗号化した状態で所有する。デバイスDV5は同様の方式で、リーフキーK0101、ノードキーK010、K01、K0、ルートキーKRを所有する。デバイスDV15も同様の方式で、リーフキーK1111、ノードキーK111、K11、K1、ルートキーKRを所有する。なお、図1のツリーにはデバイスがDV0～DV15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0037】また、図1のツリー構造に含まれる各情報処理装置（デバイス）には、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプの情報処理装置が含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図1に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0038】これらの様々な情報処理装置（デバイス）、アプリケーションが共存するシステムにおいて、例えば図1の点線で囲んだ部分、すなわちデバイスDV0、DV1、DV2、DV3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図1の点線で囲んだ部分、すなわちデバイスDV0、DV1、DV2、DV3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図1のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【0039】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によって

グループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0040】このツリー構造において、図1から明らかに、1つのグループに含まれる3つのデバイスDV0、DV1、DV2、DV3はノードキー／ルートキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイスDV0、DV1、DV2、DV3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイスDV0、DV1、DV2、DV3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーCKをノードキーK00で暗号化した値E(K00, CK)を、ネットワークを介してあるいは記録媒体に格納してデバイスDV0、DV1、DV2、DV3に配布すれば、デバイスDV0、DV1、DV2、DV3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号E(K00, CK)を解いてコンテンツキーCKを得ることが可能となる。

【0041】また、ある時点において、デバイスDV3の所有するキーK0011、K001、K00、K0、KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイスDV0、DV1、DV2、DV3のグループ）で送受信されるデータを守るために、デバイスDV3をシステムから切り離す必要がある。そのためには、ノードキーK001、K00、K0、ルートキーKRをそれぞれ新たな鍵K(t)001、K(t)00、K(t)0、K(t)Rに更新し、デバイスDV0、DV1、DV2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。もちろんコンテンツ配信に際して、他の事情、例えば著作権者側の要望やシステム配信上の都合などの各種事情に応じて、ノードキーやルートキーKRを更新する場合もある。これらのことから、正規のデバイスに対してキー更新を伝える必要がある。

【0042】更新キーの配布処理について説明する。キーの更新は、例えば、図2(a)に示す有効化キーブロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルを、たとえばネットワーク、あるいは記録媒体に格納してデバイスに供給することによって実行される。例えば上記のようにデバイスDV3を切り離す場合は、EKBをデバイスDV0、DV1、DV2に供給する。なお、有効化キーブロック（EKB）は、図1に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化

キーブロック (EKB) は、キー更新ブロック (KRB: Key Renewal Block) と呼ばれることもある。

【0043】図2(a)に示す有効化キーブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図2の例は、図1に示すツリー構造中のデバイスDV0, DV1, DV2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。例えば上記のようにキーK0011, K001, K00, K0, KRが不正に露呈された場合を想定すると、デバイスDV0, デバイスDV1は、更新キーとしてK(t)00, K(t)0, K(t)Rが必要となり、デバイスDV2は、更新キーとしてK(t)001, K(t)00, K(t)0, K(t)Rが必要となる。

【0044】図2(a)のEKBに示されるように、この場合EKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、E(K0010, K(t)001)である。これはデバイスDV2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイスDV2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図2(a)の下から2段目の暗号化キーE(K(t)001, K(t)00)を復号可能となり、更新ノードキーK(t)00を得ることができる。以下、図2(a)の上から2段目の暗号化キーE(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0を得、さらに上から1段目の暗号化キーE(K(t)0, K(t)R)を復号し更新ルートキーK(t)Rを得る。

【0045】一方、デバイスDV0, DV1においてそれぞれリーフキーK0000, K0001、及びノードキーK000は更新する対象に含まれておらず、更新キーとして必要なのは、K(t)00, K(t)0, K(t)Rである。このためデバイスDV0, DV1では、それぞれ図2(a)の上から3段目の暗号化キーE(K000, K(t)00)を復号して更新ノードキーK(t)00を取得し、また暗号化キーE(K(t)00, K(t)0)を復号して更新ノードキーK(t)0を取得し、さらに暗号化キーE(K(t)0, K(t)R)を復号して更新ルートキーK(t)Rを得る。このようにして、デバイスDV0, DV1, DV2は更新したルートキーK(t)Rを得ることができる。なお、図2(a)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0046】また、図1に示すツリー構造の上位段のノードキーK(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図2(b)の有効化キーブロック (EKB) を用い

ることで、更新ノードキーK(t)00をデバイスDV0, DV1, DV2に配布することができる。

【0047】図2(b)に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイスDV0, DV1, DV2, DV3がある記録媒体を用いており、新たな共通のコンテンツキーCK(t)が必要であるとする。このとき、デバイスDV0, DV1, DV2, DV3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新コンテンツキーCK(t)を暗号化したデータE(K(t)00, CK(t))を図2(b)に示すEKBとともに配布する。この配布により、デバイスDV4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。すなわち、デバイスDV0, DV1, DV2はEKBを処理して得たK(t)00を用いて上記暗号文を復号すれば、t時点でのコンテンツキーCK(t)を得ることが可能になる。

【0048】以上のようにキー構造がツリー構造とされるときも、上記例のようなEKBによって任意に各キーを更新することが可能となる。このキー構造を用いることで、各種事情に応じてルートキーKRやノードキーを更新することも容易に可能となり、正規な状態でのコンテンツ配信がフレキシブルに実行できる。

【0049】図3に有効化キーブロック (EKB) のフォーマット例を示す。4バイトでノードキーの数が示される。4バイトでノードキーの深さが示される。これは有効化キーブロック (EKB) の配布先のデバイスに対する階層ツリーの階層数を示す。4バイトでEKBのバージョンが示される。なおバージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。リザーブは予備領域である。

【0050】オフセットアドレスとして16バイトの位置から、16×Mバイトの領域にEKBの実内容となる暗号化されたノードキー (1又は複数) が示される。つまり図2(a)(b)で説明したような暗号化キーである。さらに、暗号化EKBバージョンや、電子署名 (Signature) が示される。電子署名は、有効化キーブロック (EKB) を発行したEKB発行局、例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック (EKB) 発行者が発行した有効化キーブロック (EKB) であることを確認する。

【0051】2. システム構成

上記のキー構造を採用した本発明の実施の形態について、以下説明していく。図4にシステム構成例を示す。本発明のデータ転送装置に相当するのは一次記録媒体側機器1であり、本発明のデータ記録装置に相当するのは二次記録媒体側機器20Aである。そして一次記録媒体

側機器 1 と二次記録媒体側機器 20A によりデータ転送システムが構築される。

【0052】一次記録媒体側機器 1 は、例えばパーソナルコンピュータにより形成される。以下、説明の便宜上、一次記録媒体側機器 1 をパーソナルコンピュータ 1 と表記する場合もある。ただし一次記録媒体側機器 1 は、必ずしもパーソナルコンピュータによって形成されるものではない。この一次記録媒体側機器 1 は、例えばパーソナルコンピュータ上で起動される SDMI コンテンツデータの蓄積／転送等を実行するソフトウェアによって、本発明でいうデータ転送装置としての動作を実行する。そしてパーソナルコンピュータ 1 に内蔵（又は外付け）の HDD 5 が一次記録媒体（及び一次記録媒体ドライブ手段）とされる。なお実施の形態の説明では HDD 5 を一次記録媒体とするが、もちろん一次記録媒体に相当する記録メディアは HDD に限られず、例えば光ディスク、光磁気ディスク等のメディア、機器内蔵の半導体メモリ、可搬型の半導体メモリ（メモリカード等）など、各種のものが考えられる。

【0053】一次記録媒体側機器 1 は、通信ネットワーク 110 を介してコンテンツサーバ 91 と通信可能とされ、これによって音楽等のコンテンツデータのダウンロードが可能とされる。もちろんコンテンツサーバ 91 は複数存在し、パーソナルコンピュータ 1 のユーザーは多様なデータダウンロードサービスを任意に利用できるものである。コンテンツサーバ 91 からパーソナルコンピュータ 1 にダウンロードされるコンテンツデータとしては、SDMI 準拠のコンテンツデータもあれば、SDMI に準拠していないコンテンツデータもある。

【0054】ネットワーク 110 を形成する伝送路は、有線又は無線の公衆回線網とされてもよいし、パーソナルコンピュータ 1 とコンテンツサーバ 91 の専用回線としてもよい。具体的にはネットワーク 110 としては、例えばインターネット、衛星通信網、光ファイバー網、その他各種の通信回線が適用できる。

【0055】また、パーソナルコンピュータ 1 の HDD 5 には、内蔵或いは外付けのディスクドライブ装置により CD-DA や DVD などのパッケージメディア 90（以下、ディスク 90 ともいう）から再生された音楽等のコンテンツデータを蓄積させることもできる。

【0056】パーソナルコンピュータ 1 には、二次記録媒体側機器 20A 又は 20B を接続し、この二次記録媒体側機器 20A 又は 20B に対して、HDD 5 に蓄積したコンテンツデータを転送可能とされる。二次記録媒体側機器 20A 又は 20B は、二次記録媒体に対する記録装置（記録再生装置）とされる。そしてパーソナルコンピュータ 1 から転送されてきたコンテンツデータを二次記録媒体にコピー記録できるものとされる。

【0057】二次記録媒体側機器 20A、20B の具体例としては各種考えられるが、ここでいう二次記録媒体

側機器 20B は、SDMI 対応の記録装置である。この SDMI 対応の記録再生装置 20B では、二次記録媒体として、例えばフラッシュメモリ等の半導体メモリを利用した SDMI 対応のメモリカードが想定される。従って二次記録媒体側機器 20B とは、例えば SDMI 対応のメモリカードに対する記録再生装置となる。この場合、二次記録媒体には SDMI コンテンツが暗号化された状態で記録されるものとなる。また SDMI 対応の二次記録媒体には SDMI コンテンツの識別子となるコンテンツ ID を格納する管理情報フォーマットが形成されている。パーソナルコンピュータ 1 では HDD 5 にコンテンツデータを格納する際に、そのアプリケーションによってコンテンツ ID が発生され、コンテンツデータと共に HDD 5 に格納される。またチェックアウト／チェックインの管理もコンテンツ ID を用いて行われるが、SDMI 対応の二次記録媒体では、コンテンツデータを記録する場合には当該コンテンツ ID も記録できるものとされる。

【0058】一方、二次記録媒体側機器 20A は、SDMI 対応ではないデータ記録装置に相当し、詳しくは後述するが、著作権保護が要求される SDMI コンテンツを、暗号化を解いた状態で二次記録媒体に記録するものである。ここでの二次記録媒体の例としては、ミニディスクを挙げる。従って二次記録媒体側機器 20A は、ミニディスク記録再生装置とされる。以下、二次記録媒体側機器 20A を、記録再生装置 20A と表記する場合もある。この場合、SDMI コンテンツを非暗号化状態で記録することによっても著作権保護機能が損なわれないように、後述する認証等がコピーの条件とされる。またこの場合のミニディスク等の二次記録媒体（つまり従来より普及しているメディア）には、コンテンツ ID を格納する領域が用意されていない。このため後述するが、コンテンツ ID については、特別な管理方式が採られる。

【0059】なお、二次記録媒体側機器 20A が記録再生するメディアはミニディスク以外にも、例えばフラッシュメモリ等の半導体メモリを利用したメモリカードや、光磁気ディスクとしてのミニディスク、或いは CD-R（CD Recordable）、CD-RW（CD Rewritable）、DVD-RAM、DVD-R、DVD-RW などが考えられる。従って、二次記録媒体側機器 20A としては、これらのメディアに対応する記録装置であればよい。

【0060】パーソナルコンピュータ 1 と二次記録媒体側機器 20A 又は 20B とは、例えば USB（Universal Serial Bus）、IEEE 1394 などの伝送規格に基づく接続が行われる。もちろん他の伝送規格の有線伝送路、或いは無線伝送路によりコンテンツデータ等の転送が可能とされるものでもよい。

【0061】3. SDMI コンテンツのデータパス
例えば図 4 のようなシステムを想定した場合の、SDM

Iで策定されたデータパスを図5に示す。なお、このデータパスは、例えば一次記録媒体としてのHDD5を備えたパーソナルコンピュータ1において、音楽コンテンツの蓄積及び外部機器（二次記録媒体側機器20A、20B）への転送処理についてのデータパスであり、換言すればパーソナルコンピュータ1において音楽コンテンツの蓄積／転送処理を行うソフトウェアにより実現されるものである。図5のデータパス上の手順／処理はDP1～DP9の符号を付しており、以下の説明では対応箇所をこの符号で示す。

【0062】図4に示したネットワーク110を介して外部サーバ91から配信されたコンテンツデータ（ネットワークコンテンツ）は、まずそれがSDMIに準拠した著作権保護されるコンテンツであるか否かが確認される（DP1）。配信されるネットワークコンテンツとしては、サーバ側がSDMIに準拠したコンテンツとして送信してくるもの（以下、SDMI準拠コンテンツ）と、SDMIとは無関係なコンテンツ（以下、非SDMIコンテンツ）がある。

【0063】そしてSDMI準拠コンテンツの場合は、そのデータは例えばDES等の鍵暗号によって、コンテンツ鍵CKで暗号化されている。コンテンツデータ自体は、元々はATRAC3などの圧縮方式でエンコードされたデータ（A3D）であるとする、SDMI準拠コンテンツは、E（CK，A3D）の状態配信される。

【0064】配信されたネットワークコンテンツがSDMI準拠コンテンツであった場合は、一次記録媒体であるHDD5にSDMIコンテンツとして蓄積される（DP1→DP2）。この場合、コンテンツデータは配信されたE（CK，A3D）の状態HDD5に書き込まれる。或いは、暗号化が一旦復号された後、別の鍵CK'で暗号化が行われ、つまり鍵の掛け替えが行われて、E（CK'，A3D）の状態HDD5に書き込まれることもある。

【0065】一方、ネットワークコンテンツが非SDMIコンテンツであった場合は、ウォーターマークチェック、即ち電子透かしによるスクリーニング処理が行われる（DP1→DP3）。さらに、例えばパーソナルコンピュータ1に装備されているCD-ROMドライブ等の内蔵ドライブ、或いはパーソナルコンピュータ1と接続されたディスクドライブ装置において再生されるCD-DA、DVD等のパッケージメディアから読み出されたコンテンツデータ（ディスクコンテンツ）については、直接ウォーターマークチェックが行われる（DP3）。つまりSDMIに準拠していないコンテンツデータについては、ウォーターマークチェックが行われることになる。

【0066】もしウォーターマークチェックに合格しない場合は、そのコンテンツデータはSDMIデータパス上でコピー不可扱いとなる（DP3→DP5）。具体的

な扱いはソフトウェア設計により多様に考えられるが、例えばHDD5には格納するが、他のメディアへのコピー／ムーブのための転送が不可能なコンテンツデータと扱われるようにしたり、或いはSDMI準拠のコンテンツ処理上においてHDD5に格納されないものとする事が考えられる。

【0067】ウォーターマークチェックに合格した場合、即ち電子透かしが存在し、かつコピーコントロールビットとしてコピー許可が確認された場合は、合法的にコピー可能なコンテンツデータと判断され、続いてそのコンテンツデータをSDMI扱いとするか否かが確認される（DP4）。このようなコンテンツデータをSDMIに準拠したものとして扱うか否かは、ソフトウェア設計やユーザー設定などに応じたものとすればよい。

【0068】SDMI扱いとしない場合は、非SDMI扱いとして当該SDMIに準拠したコンテンツデータパスからは除外される（DP6）。例えばSDMIに対応しない記録装置への転送等を可能としてもよい。一方、SDMI扱いとする場合は、そのコンテンツデータは暗号化され、SDMIコンテンツとしてHDD5に蓄積される（DP4→DP2）。例えばE（CK，A3D）の状態、又はE（CK'，A3D）の状態HDD5に蓄積される。

【0069】以上のデータパスにより、一次記録媒体としてのHDD5には、ネットワーク110を介して得られたSDMI扱いのコンテンツ（SDMIネットワークコンテンツ）や、CD-DAなどのディスク或いは他のメディアから取り出したSDMI扱いのコンテンツ（SDMIディスクコンテンツ）が蓄積されるものとなる。またSDMIコンテンツについては、コンテンツ毎の後述するUsage Ruleの管理などのために、コンテンツ毎にユニークなデータとなるコンテンツIDが生成され、HDD5に記憶される。

【0070】HDD5に格納されたSDMIコンテンツ（SDMIネットワークコンテンツ又はSDMIディスクコンテンツ）は、所定のルールのもとで、SDMI対応の記録再生装置20Bに対して転送し、SDMI対応の二次記録媒体にコピー可能とされる。また本例の場合はSDMI対応の記録再生装置20B以外に、記録再生装置20Aにも、所定の条件の下で転送可能となる。

【0071】まず、HDD5を有するパーソナルコンピュータ1にSDMI対応の記録再生装置20Bが接続されている場合は、以下になる。SDMIディスクコンテンツの場合は、SDMIディスクコンテンツに対応する転送の扱いのルール（Usage Rule）が決められており、その扱いルールのもとで、SDMI対応の記録再生装置20Bに対してコピーのための転送が認められる（DP8）。なおこのデータパスにおいて、一次記録媒体（HDD5）からSDMI対応記録再生装置20B（又は20A）で記録再生される二次記録媒体（メモリ

カード等) に対してのコピー転送が「チェックアウト」であり、逆に二次記録媒体からの一次記録媒体へのムーブ転送が「チェックイン」である。なお二次記録媒体から一次記録媒体へのムーブの場合は、二次記録媒体上では当該コンテンツデータは消去された状態となる。

【0072】SDMI ディスクコンテンツに対応する転送の扱いルールとしては、1つのコンテンツデータにつき例えば3回までのチェックアウトが許されるなど、所定のチェックアウト上限回数が定められている。従って、例えばSDMI 対応の3つの二次記録媒体まではコピー(チェックアウト)が許可される。またチェックインが行われた場合は、そのコンテンツデータについてのチェックアウト回数が減算されるものとなる。従って、例えば3つのSDMI 対応二次記録媒体にコピーした後であっても、そのうちの1つの二次記録媒体からチェックインさせれば、そのコンテンツはさらにもう一度、SDMI 対応二次記録媒体にコピー可能とされる。つまり、常に最大3つのSDMI 対応二次記録媒体にコンテンツデータが併存することが許されるものとなる。

【0073】SDMI ネットワークコンテンツの場合も、SDMI ネットワークコンテンツに対応する転送の扱いのルール(Usage Rule)が決められており、その扱いルールのもとで、SDMI 対応の記録再生装置20Bに対してコピーのための転送が認められる(DP7)。この扱いルールとしては、上記同様にチェックアウト回数上限等が決められるものであるが、その上限回数などは、SDMI ディスクコンテンツの場合の扱いルールと同様としてもよいし、異なる回数としてもよい。例えばチェックアウト上限を1回とすることが考えられる。その場合は、1つのコンテンツデータにつき、他の1つのSDMI 対応の二次記録媒体にしかコピーできないが、その二次記録媒体からチェックインすれば、再度コピー転送が可能となる。

【0074】これらの扱いルールに従って、SDMI 対応の二次記録媒体に対してコピーするためにSDMI コンテンツが転送される場合は、その伝送線路上では暗号化状態のままデータ伝送が行われる。つまり例えば上記のE(CK, A3D)の状態又はE(CK', A3D)の状態転送される。さらに、暗号化されて伝送されてきたSDMI コンテンツを受信したSDMI 対応記録再生装置20Bでは、そのSDMI コンテンツを暗号化状態のまま二次記録媒体にコピー記録することになる。

【0075】SDMI 対応記録再生装置20Bが、二次記録媒体にコピー記録されたSDMI コンテンツを再生する場合は、二次記録媒体から読み出したコンテンツデータの暗号化を復号して再生する。つまりE(CK, A3D)の状態又はE(CK', A3D)の状態二次記録媒体に記録されたコンテンツデータを、鍵CK、又は鍵CK' による復号処理を行う。即ちD{CK, E(CK, A3D)} = A3D、又はD{CK', E(CK', A3D)} = A3D、として暗号解読されたATRAC3データ(A3D)として元のコンテンツデータを得る。このコンテンツデータについてはATRAC3圧縮に対する伸張処理等を行うことで、例えばオーディオデータとして復調し、音楽等の再生出力を行う。

【0076】以上のように、SDMI 準拠のコンテンツデータは、SDMI 対応の記録再生装置20Bにチェックアウトされるまでのデータバス、さらには二次記録媒体上に至るまで、暗号化が施されたデータとなっていることや、上記転送の扱いルールチェックによるコピー管理が行われることで、コンテンツデータについての適切な著作権保護が可能となる。

【0077】一方、パーソナルコンピュータ1に、記録再生装置20Aが接続されている場合は、次のような処理が採られる。なお上記のように、記録再生装置20Aは、SDMI 対応の記録再生装置20Bとは異なって、二次記録媒体としての例えばミニディスクなどに、暗号化を解いた状態で記録するものである。暗号化を解いた状態で記録することにより、そのミニディスクにコピー記録されたコンテンツデータは、一般に普及している通常のミニディスク再生装置によっても再生可能となり、これによってユーザーの利便性を向上させることができる。但し、暗号化を解いた状態で記録することは、著作権保護の点で不都合が生じる。そこで、記録再生装置20Aにコンテンツデータを転送する場合には、所定の条件を満たすことが必要とされる。

【0078】SDMI ネットワークコンテンツを記録再生装置20Aに転送して暗号化を解いた状態で二次記録媒体にコピー記録することを許可する条件としては、例えば、①記録再生装置20Aが認証OKとなったこと、②転送しようとするコンテンツデータについてコピー記録を著作権者側が認めていること、③チェックアウト/チェックインとして転送の扱いのルール(Usage Rule)を満たすことの3つとされる。この①②③の転送条件が満たされていることでSDMI 対応記録再生装置20B以外の機器に対しても、無制限なコピー転送はできず、著作権保護機能も確保される。また、転送を行う伝送路上では暗号化状態とされること(記録再生装置20A側で暗号解読を行う)でも著作権保護機能を与えることができる。

【0079】SDMI ネットワークコンテンツを記録再生装置20Aに転送する場合には、上記①②③の転送条件がチェックされる(DP9)。即ち記録再生装置20Aについて所定の認証処理が行われる。また、コンテンツデータに含まれるフラグ情報などから、著作権者側のコピー許可の意志が確認される。さらにチェックイン/チェックアウトの扱いルールが課される。

【0080】これらの条件に従って、SDMI ネットワークコンテンツを記録再生装置20Aに転送する場合は、その伝送線路上では暗号化状態のままデータ伝送が

行われる。つまり例えば上記のE (CK, A3D) の状態又はE (CK', A3D) の状態で転送される。そしてこの暗号化されたSDMI ネットワークコンテンツは、後述する図7の構成の記録再生装置20Aにおいて受信処理された後、復号処理部28で暗号化が復号され、例えば元のATrac3圧縮データ(A3D)とされる。そしてその暗号化が解かれたコンテンツデータが、図7のエンコード/デコード部24によるエンコード処理を経て記録/再生部25に供給され、ミニディスク100にコピー記録されるものとなる。

【0081】従って記録再生装置20Aが、ミニディスク100にコピー記録したSDMIコンテンツを再生する場合は、ミニディスク100から読み出したデータについて通常のミニディスクシステムでのデコード処理、つまりEFM復調、ACIRCエラー訂正、ATrac圧縮方式に対する伸張処理等を行えばよい。これは、当該コピー記録されたミニディスク100は、通常のミニディスク再生装置に装填した場合も、コンテンツデータが通常に再生できるものとなっていることを意味する。つまりユーザーは、上述したように、ミニディスク100にコピー記録したSDMI ネットワークコンテンツを、SDMI非対応の通常のミニディスク再生装置で再生させ、音楽等を楽しむことができる。

【0082】なお、図5のデータバスにおいて、DP7, DP8, DP9の扱いルールチェック等によって転送許可がされない場合は、記録再生装置20A、20Bに対する転送が行われなことはいうまでもない。

【0083】4. データ転送装置の構成例(一次記録媒体側機器/PC)

図6に、データ転送装置となる一次記録媒体側機器1の構成を示す。なお、ここで説明する例は、パーソナルコンピュータにより一次記録媒体側機器1を形成する場合であるが、同様の機能を持つ構成が専用のハードウェアにより構築されるなどにより、データ転送専用の機器として形成されてもよい。

【0084】本例の場合は、パーソナルコンピュータ1にデータ転送装置としての機能を実行させるソフトウェアプログラムがインストールされることでデータ転送装置となる一次記録媒体側機器が実現される。なお、本明細書で「パーソナルコンピュータ」又は「コンピュータ」といっているのは、いわゆる汎用コンピュータとしての広義の意味である。当該プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク(HDD)5やROM3に予め記録しておくことができる。あるいはまた、プログラムは、フロッピー(登録商標)ディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体90に、一時的あるいは永続的に格納(記録)しておくことができる。このよう

なリムーバブル記録媒体90は、いわゆるパッケージソフトウェアとして提供することができる。

【0085】なお、プログラムは、上述したようなリムーバブル記録媒体90からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部8で受信し、内蔵するHDD5にインストールすることができる。

【0086】図6のコンピュータ1は、CPU(Central Processing Unit)2を内蔵している。CPU2には、バス12を介して、入出力インタフェース10が接続されている。CPU2は、入出力インタフェース10を介して、ユーザによって、キーボードや、マウス、マイク等で構成される入力部7が操作等されることにより指令が入力されると、それに従って、ROM(Read Only Memory)3に格納されているプログラムを実行する。あるいはまた、CPU2は、HDD5に格納されているプログラム、衛星若しくはネットワークから転送され、通信部8で受信されてHDD5にインストールされたプログラム、またはドライブ9に装着された光ディスク等のリムーバブル記録媒体90から読み出されてHDD5にインストールされたプログラムを、RAM(Random Access Memory)4にロードして実行する。これにより、CPU2は、後述するSDMIコンテンツに対してのデータ転送装置としての処理を実行する。そしてCPU2は、その処理結果を、必要に応じて、例えば入出力インタフェース10を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部6から出力、あるいは通信部8から送信、さらにはHDD5に記録等させる。

【0087】本例の場合、通信部8は、図4のネットワーク110を介した各種サーバとの通信が可能とされる。即ちコンピュータ1は、外部のコンテンツサーバ91から音楽コンテンツ等のネットワークコンテンツのダウンロードが可能とされる。ダウンロードされるネットワークコンテンツは、上述したデータバスに則って、SDMI対応のコンテンツとしての処理、もしくはSDMI非対応のコンテンツとしての処理が行われ、例えば少なくともSDMI対応の処理としてはSDMIコンテンツとしてHDD5に蓄積される。HDD5に蓄積されたSDMIコンテンツは、SDMI対応の二次記録媒体側機器20B、又は認証された二次記録媒体側機器(記録再生装置)20Aに対する転送対象のコンテンツとなる。

【0088】接続部11は、二次記録媒体側機器20A、20Bとの間でデータ通信可能に接続される部位である。例えばUSBインターフェース、IEEE1394インターフェースなどの例が考えられる。もちろん他

の規格の有線インターフェースや、赤外線や電波を用いた無線インターフェースであってもよい。

【0089】なお、図5で説明したデータバスを実現するための各種処理は、それぞれ時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。また、プログラムは、1つのコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0090】5. データ記録装置の構成例（二次記録媒体側機器／記録再生装置）

二次記録媒体側機器（記録再生装置）20Aの構成例を図7に示す。この例は、記録再生装置20Aを例えばミニディスクレコーダとして構成したものである。従って二次記録媒体100は、ミニディスク（光磁気ディスク）の例となる。以下「ミニディスク100」とも表記する。なお、図7においては、二次記録媒体100としてのミニディスクに対する記録再生データの処理系、及び上記一次記録媒体側機器1からのデータ転送に対する処理系のみを示し、ミニディスク100に対する駆動系、サーボ系、再生出力系等は通常のミニディスク記録再生装置と同様であるため詳しい図示を省略している。

【0091】MD制御部（CPU）21は記録再生装置20Aにおいてミニディスク100に対しての記録再生動作の制御を行うコントローラとなる。具体的には、ミニディスク100に対する記録再生のために、回転駆動、スピンドルサーボ、フォーカスサーボ、トラッキングサーボ、スレッドサーボなどの制御、光学ヘッド／磁気ヘッドのレーザ光や磁界印加動作の制御、記録再生データのエンコード／デコード処理の制御などを行う。

【0092】記録／再生部25は、光学ヘッド、磁気ヘッド、ディスク回転駆動系、サーボ系等が備えられ、実際にミニディスク100に対してデータの記録／再生を行う部位である。

【0093】エンコード／デコード部24は、ミニディスク100に対する記録データのエンコード、及びミニディスク100から再生された再生データのデコードを行う。公知のようにミニディスクシステムの場合は、記録データはACIRCエラー訂正符号のエンコード処理やEFM変調処理が施される。エンコード／デコード部24は、記録データに対してACIRCエンコード及びEFMエンコードを行って記録／再生部25に供給することになる。また再生時には、記録／再生部25から読み出されて供給されてきたデータ（RF信号）に対して二値化処理、EFM復調、ACIRC方式のエラー訂正処理などのデコード処理を行うことになる。

【0094】バッファメモリ30は、ミニディスク100に対する記録データ、再生データのバッファリングを

行う。特にショックブーフ機能として知られているバッファリング機能も行う。データ記録時には、バッファメモリ30にはATrac／ATrac3方式の圧縮符号化された記録データが一旦蓄積される。そして所定データ量毎に間欠的に読み出されてエンコード／デコード部24に供給され、記録処理に供される。またデータ再生時には、ミニディスク100から読み出され、エンコード／デコード部24でデコードされたデータが一旦蓄積される。そして、蓄積されたデータは連続的に読み出されてコーデック23での圧縮デコード処理に供される。

【0095】コーデック23は、ATrac／ATrac3方式の圧縮符号化による圧縮処理、及び伸張処理を行う部位である。ミニディスク100に記録されるデータは、ATrac／ATrac3方式の圧縮符号化が行われた後、上記エンコード処理が施されたものである。従って当該記録再生装置20Aに、圧縮符号化がされていないデータ、例えばPCMオーディオデータ等が記録データとして入力された場合は、コーデック23でATrac方式又はATrac3方式の圧縮符号化が行われ、その圧縮データがエンコード／デコード部24に供給されることになる。また再生時には、記録／再生部25で読み出され、エンコード／デコード部24でデコードされたデータは、ATrac／ATrac3方式の圧縮符号化状態のデータである。このデータがバッファメモリ30を介してコーデック23に供給され、コーデック23でATrac／ATrac3方式の圧縮に対する伸張処理が行われることで、例えば44.1kHz、16ビット量子化のデジタルオーディオデータが復調される。このデジタルオーディオデータは、図示しない出力系の回路において、例えばD/A変換、アナログ信号処理、増幅処理等が行われて、スピーカ出力信号とされ、音楽等として再生される。或いは、デジタルオーディオデータの状態で他の機器に対して出力可能とすることもできる。

【0096】以上の構成は、通常のミニディスクシステムの記録再生装置にも備えられる構成要素であるが、本例の記録再生装置20Aでは、一次記録媒体側機器1としてのパーソナルコンピュータに対応する部位がさらに設けられる。すなわち転送されてくるコンテンツデータについての受信・復号等の処理を行う部位として、通信部26、DMA27、復号処理部28、キャッシュメモリ29、フロー制御部31、システム制御部32が設けられる。

【0097】システム制御部32（CPU）は、当該記録再生装置20Aの全体の制御を行う部位である。例えば、パーソナルコンピュータ1との間の認証のための通信やデータ生成の指示や、パーソナルコンピュータ1からの各種コマンドのやりとり、転送されてくるコンテンツデータに対する処理などの制御を行う。またそれらの

制御に応じてMD制御部21に指示を出し、ミニディスク100に対するコンテンツデータの記録／再生、管理情報の読出や更新などの制御も行う。また図示していないが、ユーザーインターフェースとして操作部や表示部が設けられるが、操作部からのユーザー操作の監視及び操作に応じた処理や、表示部の表示制御なども行う。

【0098】通信部26は、図6のパーソナルコンピュータ1の接続部11との間で接続され、パーソナルコンピュータ1との間でデータ通信を行う部位である。例えばUSB又はIEEE1394などの通信方式に対応する信号処理を行う。通信部26によって受信されるパーソナルコンピュータ1からの通信としては、各種コマンド及びSDMIコンテンツなどがある。

【0099】通信部26で受信されたSDMIコンテンツとしてのデータは、DMA (Direct Memory Access) 27の制御により、キャッシュメモリ29に格納されていく。なおもちろん、DMA 27ではなくCPU制御によって、キャッシュメモリ29へのデータ移動を行うようにしてもよい。

【0100】復号処理部28は、SDMIコンテンツの暗号化処理に対応するための部位である。即ちキャッシュメモリ29に記憶されたコンテンツデータについての暗号解読処理を行う。そして非暗号化状態に解読したコンテンツデータは、キャッシュメモリ29の別の領域に記憶していく。

【0101】SDMIコンテンツはコンテンツキーCK又はCK'で暗号化されているため、少なくともコンテンツキーCK、CK'を認識できる情報が記憶される。具体的には後述するが、上記図1の説明で言及したDNK (Device Node Key) が記憶されることになる。この記録再生装置20Bは、図1における1つのデバイス (DVx) に相当するものとなるが、そのため、DNKにおいてリーフキーや、リーフキーによって暗号化されたノードキー、ルートキーが記憶されるものとなる。そしてそのようなDNKを用いて、また場合によっては送信されてくる上述したEKBを用いて、コンテンツキーCKを認識できる。

【0102】SDMIコンテンツに対するコンテンツキーCKを認識可能な情報であるDNKが記憶されていることで、復号処理部28は、コンテンツキーCKで暗号化された状態で送信されてきたSDMIコンテンツ、即ち例えばE (CK、A3D) の状態のコンテンツを、復号することができる。つまりD {CK、E (CK、A3D)} = A3Dとして、復号されたATRAC3圧縮状態のデータを得ることができる。このようにして復号されたATRAC3圧縮データは、エンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録できる。

【0103】なお、SDMIコンテンツは、必ずしもATRAC3圧縮データが暗号化されたものではない。例

えばリニアPCMデータが鍵CKで暗号化されたものなども考えられる。つまり例えばE (CK、PCM) の状態のコンテンツが転送入力去る場合もある。その場合は、当然ながら復号処理部でD {CK、E (CK、PCM)} = PCMとして、復号されたリニアPCMデータが得られる。その場合は、当該PCMデータは、コーデック23でATRAC3圧縮処理が行われた後、エンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録できる。

【0104】復号処理部28は、さらに認証処理のための鍵を記憶する場合もある。後述する認証処理例では記録再生装置20Aが記憶している公開鍵P、秘密鍵Sを使用する。その場合は公開鍵P、秘密鍵Sも、復号処理部28に記憶されることになる。また秘密鍵Sを用いた暗号化処理も行う。

【0105】また復号処理部28は、ハッシュエンジンも搭載しており、いわゆるハッシュ (HASH) 関数演算により、コンテンツIDを生成する処理も行う。なお、このコンテンツIDの生成については後に詳述する。

【0106】暗号化が解除されたSDMIコンテンツデータ、例えばATRAC3方式の圧縮データや、PCMデータの状態のコンテンツデータは、キャッシュメモリ29からフロー制御部31に転送されることになる。フロー制御部31は、暗号化解除されたSDMIコンテンツデータを、ミニディスク100に対して記録するために、記録処理系であるMD制御部21側 (コーデック23、エンコード／デコード部24、記録／再生部25、バッファメモリ30側) に転送する部位である。そして、MD制御部21からのリクエスト (XARQ) に応じてデータを転送していく。このフロー制御部31によって、コンテンツデータの受信、暗号解読処理、及びミニディスク100に対する記録処理の間のタイミング的な調整がはかられる。

【0107】以上の構成により、パーソナルコンピュータ1から送信されたSDMIコンテンツデータとしてE (CK、A3D) の状態のデータ、又はE (CK、PCM) の状態のデータは、非暗号化状態とされ、ATRAC3圧縮データの状態でエンコード／デコード部24でのエンコード処理を経て、記録／再生部25でミニディスク100に記録されるものとなる。

【0108】ところで、パーソナルコンピュータ1から記録再生装置20Aに対しては、コンテンツデータのチェックアウト／チェックイン、その他の通信セッションの際には、各種コマンドも送信してくる。これらのコマンドはレシーバ26によって受信されるとシステム制御部32に伝えられ、システム制御部32は、これらのコマンドに応じて各種処理を行うと共に、コマンドに対するレスポンスを通信部26からパーソナルコンピュータ1に対して送信する。

【0109】6. ミニディスクの管理方式

ここで、ミニディスク100に記録されるデータ及び管理情報について説明しておく。ミニディスクシステムのようなデジタル記録／再生システムでは、記録媒体にデータの記録動作や再生動作を制御するための管理情報としてTOC (Table of Contents) が記録されており、記録再生装置側では予めディスク等の記録媒体からこのTOC情報を読み出してメモリに保持しておき、記録再生動作の際に、このTOC情報を参照して記録位置や読出位置を把握して記録再生のためのアクセス動作を実行できるようにしている。

【0110】ミニディスクの場合、TOC情報としては書き換え不能な情報としてビットにより記録されるP-TOC (プリマスタートOC) と、楽曲等の記録、消去などに応じて書き換えられるように光磁気記録されているU-TOC (ユーザーTOC) が存在し、U-TOCについては、記録／消去に応じてまずメモリ内でデータを更新し、この更新データで所定タイミングでディスク上のU-TOC領域を書き換えていくことになる。なおU-TOCには、ディスク上に記録されるオーディオデータ等のコンテンツデータがトラックと呼ばれる単位で管理される。つまり1つのトラックは、例えば1つの楽曲に相当するものとなる。

【0111】まず、ミニディスク100に記録されるデータとして、クラスタというデータ単位について説明する。ミニディスクシステムでは記録データとして1クラスタという単位毎のデータストリームが形成されるが、この記録動作の単位となるクラスタのフォーマットは図8に示される。ミニディスクシステムでの記録トラックとしては図8のようにクラスタCLが連続して形成されており、1クラスタが記録時の最小単位とされる。

【0112】そして1クラスタCLは、セクターSCFC～SCFEとして示す3セクターのリンキングセクターと、セクターSCFFとして示す1セクターのサブデータセクターと、セクターSC00～SC1Fとして示す32セクターのメインセクターから形成されている。即ち1クラスタは36セクターで構成される。1セクタは2352バイトで形成されるデータ単位である。

【0113】リンキングセクターSCFC～SCFEは、記録動作の切れ目としての緩衝領域や各種動作調整その他に用いられ、またサブデータセクターSCFFは、サブデータとして設定された情報の記録に用いることができる。そして、TOCデータ、オーディオデータ等の記録は32セクターのメインセクターSC00～SC1Fに行なわれる。

【0114】また、セクターはさらにサウンドグループという単位に細分化され、2セクターが11サウンドグループに分けられている。つまり図示するように、セクターSC00などの偶数セクターと、セクターSC01などの奇数セクターの連続する2つのセクターに、サウンドグループSG00～SG0Aが含まれる状態となっている。

1つのサウンドグループは424バイトで形成されており、11.61msecの時間に相当する音声データ量となる。1つのサウンドグループSG内にはデータがLチャンネルとRチャンネルに分けられて記録される。例えばサウンドグループSG00はLチャンネルデータL0とRチャンネルデータR0で構成され、またサウンドグループSG01はLチャンネルデータL1とRチャンネルデータR1で構成される。なお、Lチャンネル又はRチャンネルのデータ領域となる212バイトをサウンドフレームとよんでいる。

【0115】図9はミニディスク100のエリア構造を示している。図9(a)はディスク最内周側から最外周側までのエリアを示しており、光磁気ディスクとしてのミニディスク100は、最内周側はエンボスビットにより再生専用のデータが形成されるビット領域とされており、ここにP-TOCが記録されている。ビット領域より外周は光磁気領域とされ、記録トラックの案内溝としてのグループが形成された記録再生可能領域となっている。この光磁気領域の最内周側のクラスタ0～クラスタ49までの区間が管理エリアとされ、実際の楽曲等がそれぞれ1つのトラックとして記録されるのは、クラスタ50～クラスタ2251までのプログラムエリアとなる。プログラムエリアより外周はリードアウトエリアとされている。

【0116】管理エリア内を詳しく示したものが図9(b)である。図9(b)は横方向にセクター、縦方向にクラスタを示している。管理エリアにおいてクラスタ0, 1はビット領域との緩衝エリアとされている。クラスタ2はパワーキャリブレーションエリアPCAとされ、レーザー光の出力パワー調整等のために用いられる。クラスタ3, 4, 5はU-TOCが記録される。U-TOCの内容について詳しくは後述するが、1つのクラスタ内の32個の各メインセクター(SC00～SC1F)においてデータフォーマットが規定され、それぞれ所定の管理情報が記録される。即ちプログラムエリアに記録されている各トラックのアドレス、フリーエリアのアドレス等が記録され、また各トラックに付随するトラックネーム、記録日時などの情報が記録できるようにU-TOCセクターが規定されている。このようなU-TOCデータとなるセクターを有するクラスタが、クラスタ3, 4, 5に3回繰り返し記録される。クラスタ47, 48, 49は、プログラムエリアとの緩衝エリアとされる。なお斜線部PDは、後述するプリペイド情報の記録領域として設定することができる。

【0117】クラスタ50(=16進表記で32h)以降のプログラムエリアには、1つのクラスタ内の32個の各メインセクター(SC00～SC1F)において、楽曲等の音声データがATRACと呼ばれる圧縮形式で記録される。記録される各トラック(コンテンツデータ)や記録可能な領域は、U-TOCによって管理される。な

お、プログラム領域における各クラスタにおいて、セクターSCFFは、前述したようにサブデータとしての情報の記録に用いることができる。

【0118】図10によりU-TOCセクターについて説明する。なおP-TOCは図9で説明したようにディスク90の最内周側のビットエリアに形成されるもので、読出専用の情報である。そして、P-TOCによってディスクの記録可能エリア（レコーダブルユーザーエリア）や、リードアウトエリア、U-TOCエリアなどの位置の管理等が行なわれる。なお、全てのデータがビット形態で記録されている再生専用の光ディスクでは、P-TOCによってROM化されて記録されている楽曲の管理も行なうことができるようにされ、U-TOCは形成されない。P-TOCについては詳細な説明を省略する。

【0119】図10はU-TOCセクター0のフォーマットを示すものである。U-TOCセクターとしてはセクター0～セクター32まで設けることができる。即ち上記した1クラスタ内のメインセクターSC00～SC1Fに相当して記録されるセクターとなる。その中で、セクター1、セクター4は文字情報、セクター2は録音日時を記録するエリアとされている。これらセクター1、セクター2、セクター4については説明を省略する。

【0120】U-TOCセクター0は、記録された楽曲等のコンテンツデータ（トラック）や新たにコンテンツデータが録音可能なフリーエリアについての管理情報が記録されているデータ領域とされる。例えばミニディスク100に或る楽曲の録音を行なおうとする際には、MD制御部21は、U-TOCセクター0からディスク上のフリーエリアを探し出し、ここにデータを記録していくことになる。また、再生時には再生すべき楽曲が記録されているエリアをU-TOCセクター0から判別し、そのエリアにアクセスして再生動作を行なう。

【0121】図10のU-TOCセクター0のデータ領域（4バイト×588の2352バイト）は、先頭位置にオール0又はオール1の1バイトデータが並んで形成される同期パターンが記録される。続いてクラスタアドレス(Cluster H) (Cluster L) 及びセクターアドレス(Sector)となるアドレスが3バイトにわたって記録され、さらにモード情報(MODE)が1バイト付加され、以上でヘッダとされる。ここでの3バイトのアドレスは、そのセクター自体のアドレスである。なお、同期パターンやアドレスが記録されるヘッダ部分については、このU-TOCセクター0に限らず、P-TOCセクター、プログラムエリアでのセクターでも同様であり、セクター単位にそのセクター自体のアドレス及び同期パターンが記録されている。

【0122】続いて所定バイト位置に、メーカーコード、モデルコード、最初のトラックのトラックナンバ(First TNO)、最後のトラックのトラックナンバ(Last T

NO)、セクター使用状況(Used sectors)、ディスクシリアルナンバ、ディスクID等のデータが記録される。

【0123】さらに、ユーザーが録音を行なって記録されているトラック（楽曲等）の領域やフリーエリア等を後述するテーブル部に対応させることによって識別するため、ポインタ部として各種のポインタ(P-DFA, P-EMPTY, P-FRA, P-TNO1～P-TNO255)が記録される領域が用意されている。

【0124】そしてポインタ(P-DFA～P-TNO255)に対応させることになるテーブル部として(01h)～(FFh)までの255個のパーツテーブルが設けられ、それぞれのパーツテーブルには、或るパーツについて起点となるスタートアドレス、終端となるエンドアドレス、そのパーツのモード情報（トラックモード）が記録されている。さらに各パーツテーブルで示されるパーツが他のパーツへ続いて連結される場合があるため、その連結されるパーツのスタートアドレス及びエンドアドレスが記録されているパーツテーブルを示すリンク情報が記録できるようにされている。なおパーツとは1つのトラック内で時間的に連続したデータが物理的に連続して記録されているトラック部分のことをいう。そしてスタートアドレス、エンドアドレスとして示されるアドレスは、1つの楽曲（トラック）を構成する1又は複数の各パーツを示すアドレスとなる。これらのアドレスは短縮形で記録され、クラスタ、セクター、サウンドグループを指定する。

【0125】この種の記録再生装置では、1つの楽曲（トラック）のデータを物理的に不連続に、即ち複数のパーツにわたって記録されていてもパーツ間でアクセスしながら再生していくことにより再生動作に支障はないため、ユーザーが録音する楽曲等については、録音可能エリアの効率使用等の目的から、複数パーツにわけて記録する場合もある。

【0126】そのため、リンク情報が設けられ、例えば各パーツテーブルに与えられたナンバ(01h)～(FFh)によって、連結すべきパーツテーブルを指定することによってパーツテーブルが連結できるようになされている。つまりU-TOCセクター0におけるテーブル部においては、1つのパーツテーブルは1つのパーツを表現しており、例えば3つのパーツが連結されて構成される楽曲についてはリンク情報によって連結される3つのパーツテーブルによって、そのパーツ位置の管理が行われる。なお、実際にはリンク情報は所定の演算処理によりU-TOCセクター0内のバイトポジションとされる数値で示される。即ち、304+(リンク情報)×8(バイト目)としてパーツテーブルを指定する。

【0127】U-TOCセクター0のテーブル部における(01h)～(FFh)までの各パーツテーブルは、ポインタ部におけるポインタ(P-DFA, P-EMPTY, P-FRA, P-TNO1～P-TNO255)によって、以下のようにそのパーツの内容が示される。

【0128】ポインタP-DFA は光磁気ディスク90上の欠陥領域について示しており、傷などによる欠陥領域となるトラック部分(=パーツ)が示された1つのパーツテーブル又は複数のパーツテーブル内の先頭のパーツテーブルを指定している。つまり、欠陥パーツが存在する場合はポインタP-DFA において(01h)～(FFh)のいずれかが記録されており、それに相当するパーツテーブルには、欠陥パーツがスタート及びエンドアドレスによって示されている。また、他にも欠陥パーツが存在する場合は、そのパーツテーブルにおけるリンク情報として他のパーツテーブルが指定され、そのパーツテーブルにも欠陥パーツが示されている。そして、さらに他の欠陥パーツがない場合はリンク情報は例えば『00h』とされ、以降リンクなしとされる。

【0129】ポインタP-EMPTY はテーブル部における1又は複数の未使用のパーツテーブルの先頭のパーツテーブルを示すものであり、未使用のパーツテーブルが存在する場合は、ポインタP-EMPTY として、(01h)～(FFh)のうちのいずれかが記録される。未使用のパーツテーブルが複数存在する場合は、ポインタP-EMPTY によって指定されたパーツテーブルからリンク情報によって順次パーツテーブルが指定されていき、全ての未使用のパーツテーブルがテーブル部上で連結される。

【0130】ポインタP-FRA は光磁気ディスク90上のデータの書込可能なフリーエリア(消去領域を含む)について示しており、フリーエリアとなるトラック部分(=パーツ)が示された1又は複数のパーツテーブル内の先頭のパーツテーブルを指定している。つまり、フリーエリアが存在する場合はポインタP-FRA において(01h)～(FFh)のいずれかが記録されており、それに相当するパーツテーブルには、フリーエリアであるパーツがスタート及びエンドアドレスによって示されている。また、このようなパーツが複数個有り、つまりパーツテーブルが複数個有る場合はリンク情報により、リンク情報が『00h』となるパーツテーブルまで順次指定されている。

【0131】図11にパーツテーブルにより、フリーエリアとなるパーツの管理状態を模式的に示す。これはパーツ(03h)(18h)(1Fh)(2Bh)(E3h)がフリーエリアとされている時に、この状態がポインタP-FRA に引き続きパーツテーブル(03h)(18h)(1Fh)(2Bh)(E3h)のリンクによって表現されている状態を示している。なお上記した欠陥領域や未使用パーツテーブルの管理形態もこれと同様となる。

【0132】ポインタP-TN01～P-TN255は、ディスク90にユーザーが記録を行なった楽曲などのトラックについて示しており、例えばポインタP-TN01では第1トラックのデータが記録された1又は複数のパーツのうちの時間的に先頭となるパーツが示されたパーツテーブルを指定している。例えば第1トラックとされた楽曲がディス

ク上でトラックが分断されずに、つまり1つのパーツで記録されている場合は、その第1トラックの記録領域はポインタP-TN01で示されるパーツテーブルにおけるスタート及びエンドアドレスとして記録されている。

【0133】また、例えば第2トラックとされた楽曲がディスク上で複数のパーツに離散的に記録されている場合は、その第2トラックの記録位置を示すため各パーツが時間的な順序に従って指定される。つまり、ポインタP-TN02に指定されたパーツテーブルから、さらにリンク情報によって他のパーツテーブルが順次時間的な順序に従って指定されて、リンク情報が『00h』となるパーツテーブルまで連結される(上記、図11と同様の形態)。このように例えば2曲目を構成するデータが記録された全パーツが順次指定されて記録されていることにより、このU-TOCセクター0のデータを用いて、2曲目の再生時や、その2曲目の領域への上書き記録を行なう際に、記録再生ヘッドをアクセスさせ離散的なパーツから連続的な音楽情報を取り出したり、記録エリアを効率使用した記録が可能になる。

【0134】ところで、各パーツテーブルには1バイトのトラックモードが記録されるが、これはトラックの属性情報となる。1バイトを構成する8ビットを、d1(MSB)～d8(LSB)とすると、このトラックモードは次のように定義されている。

d1・・・0:ライトプロテクト(上書き消去、編集禁止)

1:ライトパーミット

d2・・・0:著作権有り、1:著作権無し

d3・・・0:オリジナル、1:第1世代以上

d4・・・0:オーディオデータ、1:未定義

d5, d6・・・01:ノーマルオーディオ、その他:未定義

d7・・・0:モノラル、1:ステレオ

d8・・・0:エンファシスオフ、1:エンファシスオン

【0135】以上のように、書換可能な光磁気ディスク90については、ディスク上のエリア管理はP-TOCによってなされ、またレコーダブルユーザーエリアにおいて記録された楽曲やフリーエリア等はU-TOCにより行なわれる。また、このようなU-TOC構造により、ミニディスク100に記録されたトラックについては、トラックの分割、複数トラックの1トラックへの連結、消去などの編集が、U-TOCを書き換えるのみで可能であることが理解される。

【0136】記録再生装置20AにおいてMD制御部21は、記録/再生部25にミニディスク100が装填された際には、まずこのTOC情報を読み出すことになり、読み出したU-TOC情報をバッファメモリ30の特定のエリアに記憶させる。そして以後そのミニディスク100に対する記録/再生/編集動作の際に参照でき

るようにしている。なお、コンテンツデータ（トラック）の記録や、記録されているトラックの編集などが行われる場合、U-TOCセクターの更新処理は、一旦バッファメモリ30に記憶されたU-TOCデータに対して行われる。そして所定時点でバッファメモリ30に記憶されている（更新された）TOC情報がミニディスク100に書き込まれることで、ディスク上でのU-TOC更新が行われる。

【0137】7. 認証処理

SDMIデータパスの説明において言及したように、ミニディスク100に対して暗号化を解いた状態でコンテンツデータを記録する記録再生装置20Aについては、その転送/記録（チェックアウト）の条件の一つとして、パーソナルコンピュータ1からの認証がOKとならなければならない。認証とは、非暗号化状態でのコンテンツデータの記録動作が許可された機器として正当なものであるかを確認する処理となる。

【0138】この認証処理は、パーソナルコンピュータ1の接続部11に、SDMI対応記録再生装置20B以外の記録再生装置が接続された場合に行われる。なお、SDMI対応記録再生装置20Bが接続された場合は、その機器が本例でいうSDMI対応の記録再生装置20Bであることを確認する処理が行われる。即ち接続機器が、SDMI対応の記録再生装置20Bと確認されなかった場合に、以下説明する認証処理が行われ、記録再生装置20Aであるか否かが確認されるものとなる。

【0139】本例での認証処理は、非対称暗号（公開鍵暗号）を用いた認証方式を実行するものとしている。非対称暗号では、暗号化の鍵と復号化の鍵が異なる。いま、暗号前のデータをD_b、暗号鍵をK_e、復号鍵をK_dとすると、暗号化データCは、 $C = E(K_e, D_b)$ で暗号化が行われ、また $D(K_d, C) = D_b$ でデータD_bが復号される。ここで暗号鍵K_e、復号鍵K_dは鍵のペアと呼ばれ、一方は公開鍵として公開し、他方は秘密鍵として所定部位に保持されるものである。以下説明する認証処理では、鍵のペアK_e、K_dのうちで公開鍵をP、秘密鍵をSとして表して説明する。上述したようにこの場合、記録再生装置20Aは、復号処理部28（又はシステム制御部32）に暗号鍵K_e、復号鍵K_dとなる、公開鍵P、秘密鍵Sを記憶していることになる。

【0140】認証処理に際しては、例えば一次記録媒体側機器（パーソナルコンピュータ）1のCPU2が、二次記録媒体側機器（記録再生装置）20Aのシステム制御部32に対して認証要求のコマンドを送信した後、CPU2（一次記録媒体側機器（パーソナルコンピュータ）1）と、システム制御部32（二次記録媒体側機器（記録再生装置）20A）の間で図12のような処理が行われることになる。

【0141】認証処理が開始されると、まず二次記録媒

体側機器20Aのシステム制御部32は、処理S1として、復号処理部28に記憶している公開鍵Pをインターフェース部26から一次記録媒体側機器1に送信させる。なお、公開鍵Pは一次記録媒体側機器1側も知っている鍵である。従って、公開鍵Pについて両者が一致した認識が得られる場合は、当該処理S1は必ずしも実行されなくてもよい。一次記録媒体側機器1のCPU2は、公開鍵Pを受信したら、続いて処理S2として、乱数rを発生させる。そして処理S3として、二次記録媒体側機器20Aに乱数rを送信する。次に二次記録媒体側機器20Aのシステム制御部32は、処理S4として受信された乱数rを、復号処理部28に記憶された秘密鍵Sを用いて暗号化する。そして処理S5として、暗号化データE(S, r)を一次記録媒体側機器1に送信する。

【0142】一次記録媒体側機器1のCPU2は、暗号化データE(S, r)を受信したら、処理S6として、暗号化データE(S, r)を、公開鍵Pにより復号する。つまりD{P, E(S, r)}の処理を行う。そして処理S7として、上記処理S2で発生させた乱数rと、上記処理S6での復号結果D{P, E(S, r)}を比較する。ここで、公開鍵Pと秘密鍵Sが適正な鍵のペアであったとすると、 $r = D\{P, E(S, r)\}$ の結果が得られるはずである。そこで、比較結果が一致していた場合は、当該二次記録媒体側機器20Aが、公開鍵Pに対する秘密鍵Sを保持していることが確認されたことになるため、処理S8から処理S9に進み、当該二次記録媒体側機器20Aを正当な接続相手として認証する。一方、比較結果が一致していなければ処理S8から処理S10に進み、接続された二次記録媒体側機器は、正当な接続相手（即ちSDMIコンテンツを転送してよい機器）ではないとして認証NGとする。

【0143】例えば以上のような認証処理により、接続された機器が、適正な二次記録媒体側機器20Aとして認証されると、一次記録媒体側機器1は、その接続された機器に対してSDMIコンテンツの転送を許可する条件の1つが満たすと認識することになる。

【0144】8. コンテンツ暗号化方式

本例のシステムにおいて、図1に示した構造の最下段のデバイスに相当するのは記録再生装置20A、20Bとなるが、図1に示したような暗号化構造を当該システムにおいて実現する場合の例を説明する。

【0145】まず図13はコンテンツデータ及びキーの流れを示している。図4に示した外部サーバ91からパーソナルコンピュータ1に或るコンテンツデータCT1が配信される場合、この1単位のコンテンツデータCT1については、E(CK, A3D)、E(KR, CK)、及びEKBが送信されてHDD5に格納されることになる。E(CK, A3D)はコンテンツキーCKで暗号化されたATRAC3圧縮コンテンツデータであ

り、つまり配信目的たる実際の音楽その他の情報である。E (KR, CK) は、コンテンツデータの暗号解読のためのコンテンツキーCKを、図1で説明したルートキーKRで暗号化した情報である。EKBは図1～図3で説明した有効化キープロックの情報であり、本実施の形態の説明においては、ルートキーKRを更新するための情報であるとする。

【0146】1つのコンテンツデータの配信に応じて、これらがセットで配信され、図示するようにHDD5には、これらのセットとしてのコンテンツデータCT1、CT2・・・が格納されるものとなる。

【0147】パーソナルコンピュータ1が記録再生装置20A又は20Bに対してコンテンツデータ転送を行う場合は、このセットとしての情報としてE (CK, A3D)、E (KR, CK)、及びEKBを、所定の手順で送信する。図1で説明したデバイス(端末)に相当する記録再生装置20A、20Bでは、それぞれ固有のリーフIDが設定されており、またDNK (Device Node Key) を記憶している。

【0148】そしてパーソナルコンピュータ1から上記セットのコンテンツデータが送信されてくことに応じて、コンテンツデータの暗号解読を行い(又は暗号化状態のまま)、二次記録媒体に記録する。SDMI対応の記録再生装置20Bの場合は、再生時において暗号解読を行うことになる。また記録再生装置20Aの場合は、記録時において暗号解読を行う。

【0149】この暗号解読の処理としては、図示するように、まず記憶しているDNKと送信されてくるEKBを用いてルートキーKRを解読する。続いて解読したルートキーKRを用いてコンテンツキーCKを解読する。そして解読したコンテンツキーCKを用いることで、暗号化を解除したコンテンツデータA3Dを得ることができる。

【0150】記録再生装置20Aの場合のDNK及び暗号解読手順を図14、図15で具体的に説明する。今、図14(a)のようなキーのツリー構造を想定し、例えば記録再生装置20Aに、リーフID=SET0、リーフキー=K000が設定されているとする。この場合、記録再生装置20Aに記憶されるDNKは、図14

(b)のような情報を有する。まずリーフIDとして「SET0」が記憶される。またリーフキーとして「K000」が記憶される。そしてリーフキー「K000」から図14(a)の構造でルートキーKRまでをたどることのできる情報が記憶される。つまり、ノードキーK00、K0、ルートキーKRが記憶される。但しこのノードキーK00、K0、ルートキーKRは、リーフキーK000によって暗号化された状態で記憶される。即ち図示するように、

E (K000, K00)

E (K000, K0)

E (K000, KR)

が記憶されるものとなる。

【0151】このようなDNKが記憶されていることで、記録再生装置20Aは、転送されてきたコンテンツデータE (CK, A3D) を、同じく転送されてきたE (KR, CK) を用いて暗号解読できる。即ちこの場合は、記録再生装置20AはリーフキーK000を用いてD {K000, E (K000, KR)} の復号を行うことでルートキーKRを得ることができる。そして復号したルートキーKRを用いてD {KR, E (KR, CK)} の復号を行うことでコンテンツキーCKを得ることができる。さらに復号したコンテンツキーCKを用いてD {CK, E (CK, A3D)} の復号を行うことで暗号解読されたコンテンツデータA3Dを得ることができる。

【0152】但し、上述したように常にルートキーKRやノードキーは不変のものではなく多様な事情により変更される。そしてこの例のようにコンテンツキーCKをルートキーKRで暗号化して転送するシステムの場合は、コンテンツデータ毎にルートキーKRを変更することもあり得る。例えば音楽配信業者によっては1つのコンテンツデータ毎にルートキーKRを変更し、これによって著作権保護を強化する場合がある。このために、上記のようにEKBを同時に送信して、正規のデバイスに対して変更したルートキーKRが確認できるようにしている。

【0153】いま、図15に示すように、或るコンテンツデータE (CK, A3D) について、変更したルートキーKR' で暗号化したコンテンツキーE (KR', CK)、及びEKBが送信されてくとする。この場合EKBには、例えばノードキーK0で暗号化した更新ルートキーKR' としてE (K0, KR') の情報が含まれていたとする。なお更新ルートキーKR' をノードキーK0で暗号化することは、例えば図14のデバイス(SET0)～(SET3)のみに対して、新たなルートキーKR' を通知する場合などに行われる例となる。もちろんデバイス(SET0)(SET1)のみを通知対象とするなら、更新ルートキーKR' をノードキーK00で暗号化したE (K00, KR') の情報が含むEKBを発行すればよい。

【0154】一方、記録再生装置20AのDNKは、図14(b)で説明したように、リーフキーK000と、リーフキーで暗号化されたノードキー及びルートキーとしてE (K000, K00)、E (K000, K0)、E (K000, KR) が記憶されている。この状態において、コンテンツデータA3Dを復号するまでの手順を図15に①～④で示している。

【0155】① EKBとしてE (K0, KR') の情報が送られてきたことに応じて、まずDNKからK0を得る。即ちリーフキーK000を用いてD {K000,

E (K 0 0 0 , K 0) } の復号を行うことでノードキー K 0 を得る。

② 次にノードキー K 0 を用いて、E K B による E (K 0 , K R ') を解読する。即ち D { K 0 , E (K 0 , K R ') } の復号を行うことで更新ルートキー K R ' を得る。

③ 解読した更新ルートキー K R ' を用いて、送信されてきたコンテンツキー E (K R ' , C K) を解読する。つまり D { K R ' , E (K R , C K) } の復号を行うことでコンテンツキー C K を得る。

④ 復号したコンテンツキー C K を用いて D { C K , E (C K , A 3 D) } の復号を行うことで暗号解読されたコンテンツデータ A 3 D を得る。

【 0 1 5 6 】 以上の手順により、記録再生装置 2 0 A では、転送されてきたコンテンツデータの暗号化を解除して、ミニディスク 1 0 0 に記録することができる。また記録再生装置 2 0 B の場合では、暗号化された状態で二次記録媒体に記録したコンテンツデータを再生する際に、上記手順によって暗号化を解除し、音楽等の再生を行うことができる。

【 0 1 5 7 】 9. 各種コマンド

一次記録媒体側機器であるパーソナルコンピュータ 1 と、二次記録媒体側機器である記録再生装置 2 0 A (2 0 B) との間では、チェックアウト/チェックイン或いは他の各種の動作のための通信セッションにおいて、各種のコントロールコマンド及びそれに対するレスポンスコマンドのやりとりが行われる。ここでは、多様なコマンドのうち、後述する本例の特徴的な動作に直接的に関連するコマンドのみについて、説明しておく。

【 0 1 5 8 】 図 1 6 にチェックアウトコントロールコマンド、図 1 7 にチェックアウトレスポンスコマンドの各フォーマットを示す。チェックアウトコントロールコマンドは 2 5 バイトで構成され、チェックアウトレスポンスコマンドは 1 7 バイトで構成される。そしてチェックアウトコントロールコマンドは、チェックアウトのための通信セッションにより二次記録媒体側に転送したコンテンツデータを、実際に二次記録媒体側が再生可能な状態とすること(再生権を与える)を指示するために、パーソナルコンピュータ 1 が記録再生装置 2 0 A (2 0 B) に対して発するコマンドとなる。一方、記録再生装置 2 0 A (2 0 B) は、これに対応して所定の処理を行い、コントロールコマンドに対する応答としてチェックアウトレスポンスコマンドをパーソナルコンピュータ 1 に送信する。

【 0 1 5 9 】 図 1 6 に示すようにチェックアウトコントロールコマンドでは、オペレーションコードとして「チェックアウト」が示され、通信結果 (result)、通信対象機器の識別コード (List ID)、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ (object position number)、暗号化セッションキー

(DES CBC (K s , 0)) としての各情報ビットが用意される。またチェックアウトレスポンスコマンドは、図 1 7 に示すように、オペレーションコードとして「チェックアウト」が示され、通信結果 (result)、通信対象機器の識別コード (List ID)、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ (object position number) としての各情報ビットが用意される。

【 0 1 6 0 】 図 1 8 に 3 0 バイトとされるレコードオブジェクトコントロールコマンド、図 1 9 に 6 2 バイトのレコードオブジェクトレスポンスコマンドの各フォーマットを示す。レコードオブジェクトコントロールコマンドは、例えばチェックアウトのための通信セッションにおいて、実際のコンテンツデータの転送に際してそのコンテンツデータの情報を通知するためなどに、パーソナルコンピュータ 1 が記録再生装置 2 0 A (2 0 B) に対して発するコマンドとなる。一方、記録再生装置 2 0 A (2 0 B) は、これに対応して通知された情報等に関する処理を行い、コントロールコマンドに対する応答としてチェックアウトレスポンスコマンドをパーソナルコンピュータ 1 に送信する。また後述するが、記録再生装置 2 0 A においては、転送されてくるコンテンツデータの一部を用いてコンテンツ ID を生成するが、レコードオブジェクトレスポンスコマンドにより、当該生成したコンテンツ ID をパーソナルコンピュータ 1 に通知することも行う。

【 0 1 6 1 】 図 1 8 に示すようにレコードオブジェクトコントロールコマンドでは、オペレーションコードとして「レコードオブジェクト」が示され、通信結果 (result)、通信対象機器の識別コード (Destination List ID)、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ (new object position number)、コンテンツデータのタイプ (content type)、一次記録媒体側のコンテンツデータフォーマット (Download Format Track Attribute)、二次記録媒体におけるコンテンツ属性 (Track Mode)、コンテンツデータのデータ長 (Content Size)、コンテンツデータのバルクデータ長 (Bulk Data Size) としての各情報ビットが用意される。一次記録媒体側のコンテンツデータフォーマット (Download Format Track Attribute) とは、HDD 5 に格納されている、送信しようとするコンテンツデータの圧縮方式及びビットレートの情報や、コンテンツデータを伝送路に送出する際のコンテンツデータの圧縮方式及びビットレートの情報である。二次記録媒体におけるコンテンツ属性 (Track Mode) とは、ミニディスク 1 0 0 に記録する際の圧縮方式の指定情報や、ステレオ・モノラルその他の属性情報である。圧縮方式としては、例えば ATRAC、ATRAC3 の 1 3 2 k b p s、ATRAC3 の 6 6 k b p s のいずれかが指定される。

【 0 1 6 2 】 これと同様に図 1 9 に示すレコードオブジ

エクトレスポンスコマンドは、オペレーションコードとして「レコードオブジェクト」が示され、通信結果 (result)、通信対象機器の識別コード (Destination List ID)、チェックアウトコンテンツについての二次記録媒体側でのトラックナンバ (new object position number)、コンテンツデータのタイプ (content type)、一次記録媒体側のコンテンツデータフォーマット (Download Format Track Attribute)、二次記録媒体におけるコンテンツ属性 (Track Mode)、コンテンツデータのデータ長 (Content Size)、コンテンツデータのバルクデータ長 (Bulk Data Size) としての各情報ビットが用意される。そしてさらにレスポンスコマンドの場合は、32バイトのセッションデータとして、記録再生装置20Aにおいて算出されたコンテンツIDの情報をパーソナルコンピュータ1に通知する領域が用意されている。コンテンツIDについては後に詳述する。

【0163】図20にチェックインコントロールコマンド、図22にチェックインレスポンスコマンドの各フォーマットを示す。チェックインコントロールコマンドは17バイトで構成され、チェックインレスポンスコマンドは25バイトで構成される。そしてチェックインコントロールコマンドは、通信セッションにより二次記録媒体側のコンテンツデータをチェックインさせる、つまり二次記録媒体側での再生権を返却させることを指示するために、パーソナルコンピュータ1が記録再生装置20A (20B) に対して発するコマンドとなる。ただし、チェックイン以外にパーソナルコンピュータ1が二次記録媒体側の固有情報を得るために発する場合もある。一方、記録再生装置20A (20B) は、チェックインコントロールコマンドに対応して所定の処理を行い、コントロールコマンドに対する応答としてチェックインレスポンスコマンドをパーソナルコンピュータ1に送信する。

【0164】図20に示すようにチェックインコントロールコマンドでは、オペレーションコードとして「チェックイン」が示され、通信結果 (result)、サブファンクション (Subfunction)、通信対象機器の識別コード (List ID)、チェックインコンテンツについての二次記録媒体側でのトラックナンバ (object position number) としての各情報ビットが用意される。

【0165】ここで、サブファンクションは図21のように定義され、これによってチェックインコマンドによる指示内容が指定される。サブファンクションの値が「00h」であれば、そのチェックインコントロールコマンドは、コンテンツIDを要求するものとなる。これは二次記録媒体側の再生権を返却させる実際のチェックインとしての指示となる。サブファンクションの値「01h」はリザーブとされる。但し実際のチェックイン処理過程における指示に用いてもよい。サブファンクションの値がそれら以外の場合は、そのチェックインコントロール

コマンドは、プリベイド情報を要求するものとなる。プリベイド情報については後述するが、これは二次記録媒体に記録された固有情報の一つである。そして、この場合は、チェックインコントロールコマンドは、あくまでプリベイド情報の読出を指示するものであって、チェックイン (再生権の返却) は行われない。なお、プリベイド情報以外に、二次記録媒体側の固有情報、例えばユーザー情報や使用状況などの情報等を要求できるようにサブファンクションの値を定義することもできる。

【0166】またチェックインレスポンスコマンドは、図22に示すように、オペレーションコードとして「チェックイン」が示され、通信結果 (result)、サブファンクション (Subfunction)、通信対象機器の識別コード (List ID)、チェックインコンテンツについての二次記録媒体側でのトラックナンバ (object position number) としての各情報ビットが用意される。そして更にHASH関数処理で形成されたコンテンツIDをパーソナルコンピュータ1側に通知するための8バイト (Hash MAC) が用意される。但し、この最後の8バイトにコンテンツIDが組み込まれて通信されるのは、上記チェックインコントロールコマンドとしてサブファンクションの値が「00h」であった場合、つまり実際にチェックインが行われる場合である。

【0167】チェックインコントロールコマンドのサブファンクションの値によりプリベイド情報が要求された場合は、図23のように最後の8バイトにおいてプリベイド情報が組み込まれて、パーソナルコンピュータ1に対して送信されることになる。

【0168】図24はイクスクルーシブログインコントロールコマンド、図25はイクスクルーシブログアウトコントロールコマンドを示している。このコマンドは、パーソナルコンピュータ1が記録再生装置20Aに対して排他的制御を行うためのコマンドである。イクスクルーシブログインコントロールコマンドでは、サブユニットタイプ (subunit type)、サブユニットID (subunit ID) により制御対象機器が示される。そしてプライオリティ (priority) の値により、制御レベルが指示される。なお、イクスクルーシブログアウトコントロールコマンドは、記録再生装置20Aに対する排他的制御を解除するためのコマンドであり、この場合はプライオリティ (priority) の値を「00h」とし、フリー状態の制御レベルであることを指示するコマンドとして形成されている。

【0169】イクスクルーシブログインコントロールコマンドにより、記録再生装置20Aは二次記録媒体 (ミニディスク100) に対するコンテンツデータの消去、編集、或いはディスク排出、電源制御などが禁止又は制限される。つまりこのコマンドは、これらの動作処理はあくまでもパーソナルコンピュータ1側から指示されるものとする状態に遷移させるコマンドである。

【0170】このイクスクルーシブログインコントロールコマンドによるプライオリティの値によっては、動作の禁止又は制限として多様な状態を設定できる。例えば、記録再生装置20Aに対して、

制御レベル4：パーソナルコンピュータ1以外の一切の指示に対応する処理を禁止する。

制御レベル3：パーソナルコンピュータ1以外の指示による電源制御、イジェクト、トラックの分割、連結、消去を禁止する。

制御レベル2：パーソナルコンピュータ1以外の指示によるトラックの分割、連結、消去を禁止する。

制御レベル1：チェックアウトコンテンツではないトラックについては編集や消去を許可する。

制御レベル0：制限無し

などのように各種状態を設定できる。もちろん、このような制御レベルの設定は一例であり、実際には制御レベルの段階数や内容は多様に考えられる。

【0171】10. コンテンツのチェックアウト／チェックイン

続いてパーソナルコンピュータ1のHDD5に格納されたコンテンツデータを記録再生装置20Aにチェックアウトさせる場合、及びチェックアウトさせたコンテンツデータをチェックインさせる場合のそれぞれについて、パーソナルコンピュータ1と記録再生装置20Aで行われる処理を説明する。なお、実際には1つの通信セッションで複数のコンテンツデータのチェックアウト／チェックインが行われることも多いが、説明の簡略化のため、1つのコンテンツデータのチェックアウト／チェックインとしての処理の流れを説明することとする。

【0172】図26、図27はチェックアウトのための処理を示している。図26、図27において、パーソナルコンピュータ1のCPU2が実行する制御処理をステップF101～F111とし、また記録再生装置20Aのシステム制御部32、復号処理部28等によって実行される制御処理をステップF201～F215として示している。なお、通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【0173】HDD5に格納されている或るコンテンツデータの転送を行う場合は、CPU2は図26のステップF101として記録再生装置20Aに対して認証処理の開始を要求する。即ち認証開始コントロールコマンドを送信する。これに対して記録再生装置20Aはパーソナルコンピュータ1に対してステップF201で認証開始許可を通知する。即ち認証開始レスポンスコマンドを送信する。

【0174】するとパーソナルコンピュータ1はステップF102としてリーフIDを要求し、これに応じて記録再生装置20AはステップF202で記憶しているリーフIDを送信する。なお、パーソナルコンピュータ1

は接続された記録再生装置20Aを、このようにリーフIDを確認して、現在有効なリーフIDの機器であるか否かを確認する。

【0175】続いて、パーソナルコンピュータ1はステップF103として、これから転送しようとするコンテンツデータについてのEKBを記録再生装置20Aに送信する。記録再生装置20Aでは、EKBが送信されてきたら、まずステップF203でEKBのバージョンナンバーを記憶する(図3参照)。さらにステップF204で、受信したEKBと、記憶しているDNKを用いて、図15で説明した手順①②のようにして、今回の転送にかかるコンテンツデータのルートキーKRを探索し、得られたルートキーKRを記憶する。そしてステップF205で、ルートキーKRの探索完了をパーソナルコンピュータ1側に通知する。

【0176】以上の処理でルートキーKRの確認が完了したことから、パーソナルコンピュータ1はステップF104として、実際のチェックアウトセッションの開始を要求する。これに対して、記録再生装置20AはステップF206でチェックアウトセッションの開始を了承する通知を行う。なお、このセッション開始のコントロールコマンド及びレスポンスコマンドの際には、図12で説明した認証処理も行われることになる。つまり、SDMI非対応であって、暗号化を解いてコンテンツデータを二次記録媒体に記録する記録再生装置20Aとして、正規なものであるか否かの認証が行われる。図26には示していないが、もちろん認証NGとなればチェックアウトセッションは中止される。

【0177】次にパーソナルコンピュータ1はステップF105で、今回転送しようとするコンテンツデータに係る、暗号化コンテンツキーE(KR, CK)を送信する。これを受けた記録再生装置20AではステップF207で上記図15の手順③のように、記憶したルートキーKRを用いて、暗号化コンテンツキーE(KR, CK)を復号し、コンテンツキーCKを解読する。そしてステップF208で、パーソナルコンピュータ1に対してコンテンツキーCKの解読完了を通知する。

【0178】続いてパーソナルコンピュータ1はステップF106で、図18により説明したレコードオブジェクトコントロールコマンドを送信し、記録再生装置20Aに対して、チェックアウトしようとするコンテンツの情報を提供する。なお、図示していないが、これに対して記録再生装置20Aはレスポンスコマンドを返す。

(この場合のレスポンスコマンドは図19の形式ではなく、図示及び説明を省略した25バイトの形式である。)

【0179】そしてコンテンツキーCKの解読完了通知及びレコードオブジェクトコントロールコマンドに対するレスポンスにより、パーソナルコンピュータ1は記録再生装置20A側でコンテンツデータ受信／解読のため

の準備が完了したことを認識できるため、次に「P1」として示すように図27のステップF107に進み、コンテンツデータの転送を実行する。即ちコンテンツキーCKで暗号化されたコンテンツデータE(CK, A3D)を送信する。記録再生装置20A側では「R1」で示すように図27のステップF209に進み、送信されてきたコンテンツデータE(CK, A3D)の受信処理、図15の手順④のようにコンテンツキーCKを用いた復号処理、及び復号されたコンテンツデータA3Dのミニディスク100への記録処理を行うことになる。さらに、詳しくは後述するが、受信され非暗号化状態に復号したコンテンツデータから、コンテンツIDを生成する処理も行う。

【0180】1つのコンテンツデータ(例えば1つの楽曲)について、パーソナルコンピュータ1からの転送及びミニディスク100への記録が完了したら、その時点でミニディスク100上のU-TOCの更新が必要になる。ミニディスク100では、上述したように例えば1曲の単位としてのトラックのスタートアドレス/エンドアドレスその他を、ディスク内周部に記録されるU-TOCにおいて管理するものであり、トラックの再生時にはU-TOCからディスク上のアドレスを把握するものであるためである。

【0181】但し本例では、1つのコンテンツデータについてのミニディスク100への記録が終了した時点では、ステップF210として示すように、バッファメモリ30上でU-TOCを更新するのみにとどめ、ミニディスク100上でU-TOCを更新することは行わない。そして、バッファメモリ30上でU-TOC更新を完了したら、ステップF211でパーソナルコンピュータ1に対して、図19で説明したレコードオブジェクトレスポンスコマンドを送信する。これにより、1つのコンテンツデータの書込に関する処理を完了し、かつ、そのコンテンツデータについてステップF209の際に生成したコンテンツIDをパーソナルコンピュータ1に通知する。

【0182】パーソナルコンピュータ1側では、コンテンツIDの通知に応じて、ステップF108としてコンテンツIDテーブルの処理を行う。これについては後述するが、これはHDD5に蓄積されたコンテンツデータに対応してパーソナルコンピュータ1側で付したコンテンツIDと、上記のステップF209における処理において記録再生装置20A側で生成されたコンテンツIDを対応させる処理となる。

【0183】次にパーソナルコンピュータ1は、ステップF109として、図17に示したチェックアウトコントロールコマンドを送信する。またパーソナルコンピュータ1は、このようにチェックアウトを行なうことに応じて、ステップF110で、当該コンテンツデータに関して扱いルール(Usage Rule)を更新する。即ち転送許

可回数としてのコンテンツ権利を1つ減算する。

【0184】記録再生装置20A側では、チェックアウトコントロールコマンドによりチェックアウトが実際に指示されたとして処理を行う。即ちステップF212で、ミニディスク100上でU-TOCを更新し、記録したコンテンツデータを再生可能な状態とする。これにより二次記録媒体上でコンテンツデータの再生権が与えられたことになる。なお、このとき、当該コンテンツデータに対応するU-TOCセクター0のトラックモードにおいて、上述したビットd1=1とされており、つまり当該コンテンツデータはライトプロテクト状態とされる。そして、記録再生装置20Aは、チェックアウトにかかるU-TOC更新を終了することに応じて、ステップF213でチェックアウトレスポンスコマンドを送信し、完了を通知する。以上でチェックアウト、つまりコンテンツ権利の譲渡が完了する。

【0185】チェックアウトの完了に応じて、パーソナルコンピュータ1はステップF111でセッション終了要求のコントロールコマンドを記録再生装置20Aに送信する。記録再生装置20AはステップF214としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ1に送信する。またパーソナルコンピュータ1はステップF112で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置20AはステップF215で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、チェックアウトのための一連の通信が終了される。

【0186】なお、このような通信により複数のコンテンツデータをチェックアウトする場合は、各コンテンツについてルートキーが共通であれば、ステップF105～F108及びF207～F211の処理が繰り返されればよい。またEKBバージョンが異なるコンテンツデータを連続して転送する場合は、コンテンツに対応してEKB転送も行えばよい。

【0187】続いてチェックインの場合の処理を図28で説明する。図28において、パーソナルコンピュータ1のCPU2が実行する制御処理をステップF101～F156とし、また記録再生装置20Aのシステム制御部32、復号処理部28等によって実行される制御処理をステップF201～F257として示している。この場合も、通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【0188】チェックインの場合も、認証開始からEKB転送、ルートキー探索等の処理は上記チェックアウトの場合と同様に行われる。即ち上記図26と同一のステップ番号を付したステップF101～F103、F201～F205は、上述と同様の処理が行われるものであり、重複説明を避ける。

【0189】パーソナルコンピュータ1はステップF150で、チェックインセッションの開始を要求するコン

トロールコマンドを送信する。これに応じて記録再生装置20AはステップF250で、レスポンスコマンドを返す。なお、この場合にも、図12で説明した認証処理が行われる。

【0190】チェックインセッションが開始され、且つ記録再生装置20Aが認証OKとなったら、パーソナルコンピュータ1はステップF151として、チェックインさせようとするコンテンツデータについてのコンテンツIDを要求する。例えば記録再生装置20Aに対してチェックインさせるコンテンツデータのミニディスク100上のトラックナンバを指定して、そのコンテンツIDを要求する。記録再生装置20Aは、これに応じて、まずステップF251で、当該指定されたコンテンツデータ(トラック)が、チェックイン可能なコンテンツデータであるか否かを判断する。この判断はトラックに対応してU-TOCに記録されている書込制御フラグの状態(トラックモードのd1)で判別できる。これについては後述する。ここで判断するチェックイン可能なコンテンツデータとは、チェックアウトされたコンテンツデータであって、しかもミニディスク100側で編集が行われていないコンテンツデータである。

【0191】チェックイン可能なコンテンツデータであれば、ステップF252で、当該コンテンツデータについてのコンテンツIDを用意する。この場合、この時点でコンテンツIDを算出するか、或いは既に算出されて記憶されているコンテンツIDを読み出す処理となる。これについても後述する。そしてステップF253で、コンテンツIDをパーソナルコンピュータ1に送信する。なお、チェックイン可能なコンテンツデータでなかった場合は、その旨をパーソナルコンピュータ1に通知し、以降はエラー処理となる。

【0192】パーソナルコンピュータ1はステップF152として、送信されてきたコンテンツIDを照合する。つまり、記録再生装置20A側で生成され送信されてきたコンテンツIDと、チェックアウト時に記録再生装置20A側で生成し、パーソナルコンピュータ1側で生成したコンテンツIDに対応させてテーブルデータとして保存したコンテンツIDの照合をとり、チェックイン対象のコンテンツデータを正しく示しているかを照合する。そして照合OKであればステップF153で実際にチェックインを指示する。照合NGであればエラー処理となる。

【0193】ステップF153のチェックイン指示は、図20で説明したチェックインコントロールコマンドを送信するものとなる。このときチェックインコントロールコマンドにおいては、サブファンクションの値は「00h」とし(図21参照)、これによって実際のチェックイン指示であることを明示する。またリストIDの値を記録再生装置20Aを指定した値とし、オブジェクトポジションナンバの値として、チェックインさせるコン

テンツデータのミニディスク100上のトラックナンバを指定するものとなる。また、チェックイン指示に応じてステップF154で、当該コンテンツデータについての扱いルール(Usage Rule)を更新する。即ち転送許可回数としてのコンテンツ権利を1つ復活させる。

【0194】記録再生装置20A側は、これに応じてステップF254で、U-TOCデータを更新する。つまりチェックイン対象となったトラックを、ミニディスク100上から消去されるようにU-TOCセクター0の内容を更新する。つまり再生不能とし、再生権を消失した状態とする。そしてステップF255で図22のチェックインレスポンスコマンドを送信する。以上でチェックイン、つまりコンテンツ権利の返却が完了する。

【0195】チェックインの完了に応じて、パーソナルコンピュータ1はステップF155でセッション終了要求のコントロールコマンドを記録再生装置20Aに送信する。記録再生装置20AはステップF256としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ1に送信する。またパーソナルコンピュータ1はステップF156で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置20AはステップF257で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、チェックインのための一連の通信が終了される。

【0196】なお、このような通信により複数のコンテンツデータをチェックインする場合は、各コンテンツIDの確認及びチェックイン指示、つまりステップF151~F154及びF251~F255の処理が繰り返されればよい。

【0197】11. コンテンツIDの生成及び管理方式
チェックアウト/チェックインにおけるUsage Ruleは、各コンテンツ毎にコンテンツIDを用いて管理される。上述したが、SDMI対応の二次記録媒体では、コンテンツIDが格納できる記録フォーマットが採られている。従って、チェックアウト/チェックインの際も、パーソナルコンピュータ1とSDMI対応の記録再生装置20Bの間では、元々パーソナルコンピュータ1側で生成したコンテンツIDにより、対象となっているコンテンツデータを特定できる。

【0198】しかしながら、従来より普及しているミニディスク100等の二次記録媒体を対象とする、記録再生装置20Aでは、これができない。つまりミニディスク100上には、チェックアウトにより記録されたコンテンツデータについてのコンテンツIDを格納しておく領域が存在しないためである。仮にU-TOCなどにおいてそのような領域を新たに規定しコンテンツIDを記録したとしても、従前の機種種のミニディスクレコーダによってU-TOC更新が行われた場合、コンテンツIDは消去されてしまう。このためミニディスク100ではコンテンツIDを管理できない。二次記録媒体側でコン

テンツIDが管理できなければ、チェックアウトは可能でもチェックインの際にはコンテンツデータの照合がとれないため、チェックイン不能となる。

【0199】そこで記録再生装置20Aでは、コンテンツデータ自体からコンテンツIDを生成する機能を備えるようにする。そしてパーソナルコンピュータ1側では、パーソナルコンピュータ1側で発生させた第1のコンテンツIDと、記録再生装置20A側で生成した第2のコンテンツIDを照合できるようにテーブルデータを用意するものとしている。

【0200】まず、記録再生装置20AによりコンテンツIDを生成する方式を説明する。コンテンツID生成においては、非暗号化状態に復号されたコンテンツデータについて、そのコンテンツデータの長さ（コンテンツサイズ）やトラック情報に加えて、コンテンツデータストリーム内の特定のデータをサンプリングしてCBC—MAC演算をする手段などがあげられる。

【0201】図29に、1つの音楽等のコンテンツデータの全体を模式的に示している。このコンテンツデータは、例えばパーソナルコンピュータ1からチェックアウトのために送信され、暗号化状態が復号され、ATRA C又はATRA C3圧縮状態のデータストリームとして示している。このコンテンツデータに対して、例えばポイントP1、P2をサンプリングポイントとして設定し、サウンドユニット（斜線部）のデータを抽出する。1つのサウンドユニットは、例えば424バイトのデータ、つまり図8で説明した1つのサウンドグループに相当するデータなどとすればよい。ただしもちろんそれに限定されない。

【0202】そして、このようにサンプリングした実際のコンテンツデータの一部を用いてコンテンツIDを算

$$\text{Content ID} = \text{CBC_MAC}(\text{Key hash}, \text{IV}, \text{Stream(P1)} // \text{Stream(P2)}) \cdots (1)$$

ここで「Key hash」は8バイトの固有鍵データである。Stream(P1)は、サンプリングポイントP1の1サウンドグループのデータ、Stream(P2)は、サンプリングポイントP2の1サウンドグループのデータである。そして//は連結を示しており、つまり「Stream(P1) // Stream(P2)」は、サンプリングポイントP1、P2の2つのサウ

$$\text{IV} = \{\text{length} // \text{TrackModeByte} // 32\text{bits Padding with Zero}\} \cdots (2)$$

この場合、4バイトのコンテンツ長length、及び1バイトのトラック情報TrackModeByteは、図18に示したレコードオブジェクトコントロールコマンドによって通知される、4バイトのコンテンツサイズ（Content Size）と1バイトのトラックモード（Track Mode）の情報を用いることができる。

【0205】このようなコンテンツID生成は、記録再生装置20Aにおいて例えば復号処理部28に搭載されるHASHエンジンによって行われるが、上記式（1）

（2）からわかるように、記録再生装置20Aは、例えばチェックアウトセッションの際には、レコードオブジ

エクトデータをサンプリングポイントで、無音データであることが多いことが予想されるコンテンツの先頭又は終端は避けるとともに、上記P1、P2のように2箇所設けることでユニークデータとしての確率を高めることができる。つまり各コンテンツデータ毎に異なる、識別子としての機能を十分に備えたコンテンツIDを算出できる。もちろんサンプリングポイントは3カ所以上としてもよい。また先頭又は終端を避ければ、1カ所であっても不十分ではない。

【0203】また、このサンプリングポイントP1、P2は、全くランダムな位置ではなく、コンテンツデータのレングス（データサイズ）に応じて設定される位置とすることで、特定のコンテンツデータについては、何度算出しても同じコンテンツIDが得られる。つまり、二次記録媒体上においてコンテンツIDを保存しておかなくてもコンテンツデータ自体が記録されていれば、サンプリングポイントが一致することで異なる時点でも同じコンテンツIDが算出できるものであり、このことは、二次記録媒体としてのミニディスク100上にコンテンツIDを記録しておく必要をなくすることができるものとなる。具体的にはサンプリングポイントP1、P2は、例えばコンテンツデータのサイズ（レングス）から1/3の位置、及び2/3の位置などとして設定されればよい。もちろん1/3の位置、2/3の位置に限らず、レングスに対して1/2の位置、1/4の位置、3/4の位置、1/5の位置、2/5の位置、3/5の位置、4/5の位置、1/6の位置、5/6の位置・・・など、レングスに対する或る相対的なポイントが規定されればよい。

【0204】コンテンツデータからハッシュ関数を用いてコンテンツIDを得る方法を下記（1）式に示す。

サウンドユニットを繋げた（424×2）バイトのデータを示している。また「IV」は8バイトのCBCモードの初期値であり、4バイトのコンテンツ長length、1バイトのトラック情報TrackModeByteを用いて次の（2）式で与えられる。

エクトコントロールコマンドを受信（図26のステップF106）することで、上記「IV」の値を算出できる。またレコードオブジェクトコントロールコマンドにおけるコンテンツサイズ（Content Size）によりコンテンツデータが転送される前に、コンテンツデータのレングスが確認できるため、コンテンツデータのレングスの例えば1/3、2/3の位置としてのサンプリングポイントP1、P2も確認できる。従って、実際にコンテンツデータの転送が開始され、サンプリングポイントP1、P2のデータが得られた時点以降は、上記式（1）の演算によりコンテンツIDを算出できるものである。

【0206】また、ミニディスク100上に記録されたコンテンツデータについては、当然ながらコンテンツデータのサイズはU-TOCセクター0のデータから算出できるため、サンプリングポイントP1、P2の位置は確認できる。またチェックアウト時にレコードオブジェクトコントロールコマンドで通知されるトラックモード(Track Mode)の情報が、U-TOCセクター0におけるトラックモードに記録されることで、U-TOCデータから上記式(2)の算出が可能となる。従って、ミニディスク100上に記録されたコンテンツデータについては、どのような時点でもコンテンツIDを算出できるものとなる。

【0207】例えばこのようにして、記録再生装置20A側ではチェックアウトされたコンテンツデータについて独自にコンテンツIDを生成することができる。ただし、これがパーソナルコンピュータ1において生成され、HDD5に格納されたコンテンツIDと対応づけられなければ適切に利用できない。上述したようにHDD5に格納されるコンテンツIDとは、パーソナルコンピュータ1側のアプリケーションにより、コンテンツデータについて生成されたものである。このアプリケーションによって求め求められたコンテンツIDは、HDD5などの一次記録媒体を有する機器側(パーソナルコンピュータ1)に固有な情報、例えば機器にインストールされたアプリケーション毎のユニークID、HDD5に格納された時間情報や乱数などで構成される。このようなパーソナルコンピュータ1側で生成された(第1の)コンテンツIDと、上記記録再生装置20A側で生成された(第2の)コンテンツIDは、図30のようなテーブルデータにより、パーソナルコンピュータ1側で対応づけられる。なお従って、該テーブルデータは、HDD5などの一次記録媒体を有する機器毎にユニークな組み合わせになる。

【0208】即ちチェックアウトセッションの際には、図27のステップF211としてのレコードオブジェクトレスポンスコマンドにより、記録再生装置20A側で生成したコンテンツIDをパーソナルコンピュータ1側に通知する。そしてステップF108として、パーソナルコンピュータ1側ではテーブルデータの処理を行う。この処理は、即ちチェックアウトのために転送するコンテンツデータについて、パーソナルコンピュータ1側のコンテンツIDと、当該コンテンツデータについて記録再生装置20A側で生成されたコンテンツIDを対応するように、図30のテーブルデータの要素を生成していく処理である。図30では3つのコンテンツデータについて、それぞれ第1、第2のコンテンツIDが対応づけられた状態を例示している。

【0209】このようなテーブルデータがパーソナルコンピュータ1側で管理される(例えばHDD5において記録/更新されていく)ことで、ミニディスク100に

対してチェックアウトされたコンテンツデータを、コンテンツIDで管理することが可能となり、即ちチェックアウト/チェックインの管理が可能となる。上記のようにミニディスク100上にはコンテンツIDを格納する領域が存在しないが、記録再生装置20A側ではミニディスク100に記録されているコンテンツデータについてはコンテンツIDを算出できる。

【0210】従ってパーソナルコンピュータ1が或るコンテンツデータをチェックインさせたい場合は、対象となるコンテンツデータについての(第2の)コンテンツIDを記録再生装置20Aに要求し、送信されてきた(第2の)コンテンツIDと、図30のテーブルデータに記憶されている(チェックアウト時に記録再生装置20A側から送信されてきた第2の)コンテンツIDとの一致を確認することで、パーソナルコンピュータ1側で(第1の)コンテンツIDで管理しているコンテンツデータのチェックイン処理ができるものとなる。これが図28のステップF151、F152、F252、F253の処理の意味である。

【0211】このようなコンテンツID管理方式により、SDMI非対応の二次記録媒体(ミニディスク100等)に対しても、本システムにおいて適切にチェックアウト/チェックインの管理、つまりコンテンツ権利の管理が可能となる。

【0212】12. チェックアウト時及びチェックイン前のコンテンツIDの生成処理
ところで、記録再生装置20A側でコンテンツIDを生成する必要がある場合とは、通常、チェックアウトに応じてコンテンツIDをパーソナルコンピュータ1に通知する場合(パーソナルコンピュータ1側で図30のテーブルデータ管理を行うようにするためにレコードオブジェクトレスポンスコマンドで送信する場合)と、チェックイン等のためにパーソナルコンピュータ1からコンテンツIDを要求された場合となる。

【0213】そして上記のようにコンテンツIDは、サンプリングポイントP1、P2で抽出したコンテンツデータの一部を用いる。このため、例えばチェックアウト時には、パーソナルコンピュータ1から転送されたコンテンツデータがミニディスク100に書き込まれた後において、サンプリングポイントP1、P2のデータを読み出し、そのデータを用いてコンテンツIDを算出するという手順が通常考えられる。またチェックインのためにパーソナルコンピュータ1からコンテンツIDを要求された場合も、その要求に応じてミニディスク100からサンプリングポイントP1、P2のデータを読み出し、そのデータを用いてコンテンツIDを算出するという手順が通常考えられる。

【0214】ただし、このような手順では、チェックアウトセッションの間にミニディスク100に対するアクセス/データ読み出しが必要となり、その分、コンテン

ツID算出に時間を要する。これはチェックアウトのための全体の通信時間を長時間化するものとなる。またチェックインのためにコンテンツIDが要求された際にも、ミニディスク100に対するアクセス/データ読み出しが必要となり、その分、コンテンツID算出に時間を要する。これもチェックインのための通信時間を長時間化させる。そこで本例では、次のような手順でコンテンツID算出を行うことで処理の効率化及び通信時間の短縮をはかる。

【0215】図31はチェックアウトセッションにおけるコンテンツID (CID) の生成にかかる処理を示している。これは図27のステップF209においてシステム制御部32及び復号処理部28で行なわれる処理である。図26のステップF106として示したように、コンテンツデータの転送直前にパーソナルコンピュータ1からレコードオブジェクトコントロールコマンドが送信されてくるが、図27のステップF209における図31のコンテンツID生成処理としては、まずステップF301として、受信したレコードオブジェクトコントロールコマンドの内容から、これから転送されてくるコンテンツデータのレングス (データサイズ) を確認する。そしてステップF302で、コンテンツデータのレングスから、コンテンツデータストリーム内におけるサンプリングポイントP1、P2としてのポイントを算出する。

【0216】ステップF303は実際に転送されてくるコンテンツデータの受信にかかる処理の開始を示している。即ち図7のブロック図において説明したように、コンテンツデータが受信され、非暗号化状態に復号され、ATRAC3データ状態でバッファメモリ30に蓄積され、さらにエンコード/デコード部24で変調され、記録/再生部25でミニディスク100に記録されていく、という処理が開始される。このようなコンテンツデータの受信/復号/バッファリング/エンコード/記録という処理過程において、コンテンツIDにかかる処理としては、サンプリングポイントP1のデータを監視している。そしてステップF304として、サンプリングポイントP1としてのサウンドユニットのデータを例えばバッファメモリ30において確認したら、当該サウンドユニットのデータを、データストリームのバッファリングとは別に、バッファメモリ30における他の領域に格納しておく。引き続き同様に監視を行い、ステップF305として、サンプリングポイントP2としてのサウンドユニットのデータを例えばバッファメモリ30において確認したら、当該サウンドユニットのデータを、データストリームのバッファリングとは別に、バッファメモリ30における他の領域に格納しておく。

【0217】ステップF306は、コンテンツデータの受信/復号/バッファリング/エンコード/記録という処理が1つのコンテンツデータに関して終了したことを

示している。コンテンツデータのミニディスク100への記録が完了したら、ステップF307で、復号処理部28におけるHashエンジンは、上記のようにバッファメモリ30において格納しておいたサンプリングポイントP1、P2のデータを読み出し、上記式(1)

(2)の演算によりコンテンツIDを生成する。そしてステップF308で、レコードオブジェクトレスポンスコマンドにコンテンツIDをセットする。このレコードオブジェクトレスポンスコマンドは、図27のステップF211としてパーソナルコンピュータ1側に送信されることになる。

【0218】つまりこの処理例では、サンプリングポイントP1、P2のデータを、ミニディスク100に書き込む前に抽出して格納しておくため、コンテンツID算出時にミニディスク100を再生状態にして該サンプリングポイントのデータをシークし、読み出す必要はない。これによりコンテンツID算出処理が非常に効率化され、チェックアウトセッション時間も短縮できる。

【0219】次に、チェックインのためにコンテンツIDが要求された際に、迅速にコンテンツIDを送信できるようにするための処理を図32に示す。コンテンツIDは、コンテンツデータ自体が記録されていることと、レングス及びトラックモードを確認できれば算出可能である。換言すれば、ミニディスク100に記録されているコンテンツデータについては、そのコンテンツデータとU-TOCセクター0の情報が読み取ればサンプリングポイントP1、P2のデータの抽出、或いはさらにコンテンツIDの算出が可能である。

【0220】そこで図32(a)の処理では、記録再生装置20Aに対して、ミニディスク100が装填された際、或いはミニディスク100が装填されている状態で電源オンとされた場合など、つまりTOCデータ読出を行う時点で、サンプリングポイントP1、P2のデータを抽出してしまう処理を行うようにしている。

【0221】即ちステップF401としてTOC読出を行ったら、ステップF402で変数 $n=1$ としてステップF403に進み、まずトラック# n (# n はトラックナンバ、つまり最初は第1トラック) について、サンプリングポイントP1、P2を算出する。U-TOCセクター0の情報が読み込まれていることで、各トラックについてのサンプリングポイントP1、P2の算出は可能である。そしてステップF404で、トラック# n についてのサンプリングポイントP1、P2のデータを、実際にミニディスク100から読出、バッファメモリ30において特別に用意された領域に格納する。

【0222】ステップF405では、変数 n が最後のトラックナンバであるか否かを判別し、最後のトラックナンバでなければステップF406で変数 n をインクリメントしてステップF403に戻る。そしてトラック# n (即ち続いて第2トラック) についてのサンプリングポ

イントP1、P2を算出し、実際にサンプリングポイントP1、P2のデータを読み込んでバッファメモリ30に格納するという処理を行う。つまりステップF403～F406のループ処理により、ミニディスク100に収録されている全トラックについて、それぞれレングスから算出されるサンプリングポイントP1、P2のデータを読み出、バッファメモリ30に格納しておくものである。全トラックについて処理を終えたらステップF405から終了する。

【0223】一方、図28のステップF151のように、パーソナルコンピュータ1からコンテンツIDを要求された場合の処理、つまり図28のステップF252の処理は、図32(b)のようになる。即ち、ステップF451で、要求にかかるトラックナンバのトラックについてのサンプリングポイントP1、P2のデータをバッファメモリ30から読出、ステップF452で復号処理部28のHashエンジンによりコンテンツIDを算出する。なおコンテンツIDの算出のために上記式(1)

(2)で必要なトラックモードやレングスは、その時点で既にバッファメモリ30に格納されているU-TOCデータから判別できる。そしてステップF453でレスポンスコマンドに生成したコンテンツIDをセットする。このレスポンスコマンドは、図28のステップF253としてパーソナルコンピュータ1に送信されることになる。

【0224】このような処理とすることで、パーソナルコンピュータ1からコンテンツIDを要求された時点において、ミニディスク100からサンプリングポイントP1、P2のデータを読み出すという必要はないため、コンテンツID要求に対応する処理を迅速化できる。全体的にみれば、チェックインセッションとしての通信時間を短縮化できる。

【0225】ところで、図32に代えて図33の処理が行われるようにしてもよい。なお、図33において図32と同一の処理は同一のステップ番号を付し説明を省略する。図33(a)の処理としては、ステップF403としてトラック#nのサンプリングポイントP1、P2を算出したら、ステップF410としてサンプリングポイントP1、P2のデータをミニディスク100から読出す。そしてそのデータは復号処理部28のHashエンジンに供給し、ステップF411としてコンテンツIDの算出を実行する。そして算出したコンテンツIDをバッファメモリ30に格納する。

【0226】このような処理をミニディスク100に収録されている全トラックに対して行う。つまり予めコンテンツIDの生成までをも行って、バッファメモリ30に格納しておくものとなる。

【0227】そしてパーソナルコンピュータ1からコンテンツIDを要求された場合の処理、つまり図28のステップF252の処理は、図33(b)のようになる。

即ち、ステップF461で、要求にかかるトラックナンバのトラックについてのコンテンツIDをバッファメモリ30から読出、読み出したコンテンツIDをステップF462でレスポンスコマンドにセットする。このレスポンスコマンドは、図28のステップF253としてパーソナルコンピュータ1に送信されることになる。

【0228】このような処理とする場合、パーソナルコンピュータ1からコンテンツIDを要求された時点において、ミニディスク100からサンプリングポイントP1、P2のデータを読み出す処理や、コンテンツID算出処理は必要はないため、コンテンツID要求に対応する処理をさらに迅速化できる。

【0229】なお、図32(a)又は図33(a)の処理は、記録再生装置20Aにおいてミニディスク100からTOC読出を行う場合に実行されればよいが、例えば再生動作中或いは動作停止中など、空き時間を利用して処理を行うようにしてもよい。再生動作中としては、ミニディスクシステムでは、ディスクからのデータ読出は高速レートで間欠的に行うものであるため、間欠的な読出中断時間に、サンプリングポイントP1、P2のデータの読出を実行するようにすればよい。いずれにしても、パーソナルコンピュータ1からのコンテンツID要求に先だって図32(a)又は図33(a)の処理が行われていることで、チェックインセッションの効率化が実現できる。

【0230】13. コンテンツ書込制御フラグ
図26、図27のチェックアウトが行われた場合、ミニディスク100側では、当該チェックアウトコンテンツについては、U-TOCセクター0のトラックモードにおけるd1ビットが「1」とされることは先に述べた。このd1ビットは、ミニディスク100上に記録されたチェックアウトコンテンツについての書込制御フラグとして機能するものとなる。

【0231】d1ビットは、ミニディスクシステムにおいていわゆるライトプロテクトフラグとなる。つまりd1ビットがたてられたトラックは、消去や分割、連結などの編集が禁止される。つまり現在普及している従前のミニディスクレコードであれ、上記記録再生装置20Aとしてのミニディスクレコードであれ、d1ビットがたてられたトラックについては消去や分割等の編集は、行われない。ただし、実際にはミニディスクシステムにおいては、ミニディスク100上に記録されたトラックについて自動的にd1ビットがたてられることはない。従って、d1ビットは、そのトラックが編集禁止とされるだけでなく、パーソナルコンピュータ1からチェックアウトされたコンテンツであることを明示する情報となる。

【0232】本例のシステムでは、このd1ビットを書込制御フラグとして、チェックアウトコンテンツの編集を禁止するとともに、チェックイン要求の際に、そのト

ラックがチェックアウトされたものであるか否かの判別に用いるようにしている。

【0233】チェックアウトされたコンテンツデータをチェックインするには、コンテンツデータの内容が一致していることが管理上好適である。また上記のように記録再生装置20Aではコンテンツデータのレングスに基づいたサンプリングポイントP1、P2のデータを用いてコンテンツID算出を行うものであるため、もし分割或いは連結などが行われてコンテンツデータ自体のデータ長が変化してしまえば、チェックアウト時と同じコンテンツIDが生成できなくなってしまう。換言すれば、チェックアウトコンテンツが編集された場合は、コンテンツIDの不一致により適切なUsage Rule管理ができなくなり、システム処理上、チェックインを許容できないし、さらに編集により内容が変化したコンテンツデータについてチェックインを認めることは、Usage Rule管理の理念上でも適切ではない。このため、チェックアウトコンテンツについては、ミニディスク100上では編集できないようにすることが好適である。

【0234】図34に、書込制御フラグに関する記録再生装置20Aの処理を示している。なお図中「WPF」は書込制御フラグ、つまりU-TOCセクター0のトラックモードのd1ビットのことである。チェックアウトされてミニディスク100に記録されたコンテンツについては、図27のステップF212のU-TOC更新処理において、書込制御フラグWPFがオンとされる(S100)。一方、本システムにおけるチェックアウトではなく、他のソースから記録再生装置20Aもしくは他のミニディスクレコーダによってミニディスク100に記録されたコンテンツデータ(以下、自己録音コンテンツ)については、書込制御フラグWPFはオフとされたままである(S105)。

【0235】ここで、書込制御フラグWPFがオンのコンテンツデータ(トラック)については、後のチェックインを可能とするために一切の編集を禁止するという管理手法が考えられる。但し、ユーザーにチェックインができなくなることを警告した上で編集を許可するという管理手法も考えられる。

【0236】まず、チェックアウトコンテンツについての一切の編集を禁止する場合は、ユーザー操作その他により、当該コンテンツデータに対する編集指示があっても、システム制御部32は、編集禁止として、編集指示を受け付けない処理を行う(S101)。従って、チェックアウトコンテンツについては、一切編集ができないものとされ、また書込制御フラグWPFは常にオンの状態となっている(S101→S104)。

【0237】一方、自己録音コンテンツについては、もちろん自由に編集可能である(S106)。システム制御部32は、ユーザー操作その他により編集指示があれば、それに応じてMD制御部21にU-TOC更新処理

を指示し、編集を実行させればよい。但し、編集が行われようといわれまいと、自己録音コンテンツに関しては常に書込制御フラグWPFはオフである(S105→S104、又はS105→S106→S104)。

【0238】チェックアウトコンテンツについて、上記のように警告を発した上で編集を許可する場合、ユーザー操作その他により編集指示があった場合は、システム制御部32はまず図7には示していない表示機能により警告としてのメッセージ出力を行う(S102)。つまり、編集することでチェックインができなくなることを警告する。これに応じてユーザーが編集指示をキャンセルした場合は、当然編集は実行されない(S102→S104)。一方、警告後さらにユーザーが編集指示を行った場合は、ユーザーがチェックイン不可となることを納得したとして編集を許可する。即ちシステム制御部32は、ユーザー操作その他の編集指示に応じてMD制御部21にU-TOC更新処理を指示し、編集を実行させる。このとき、編集にかかるトラックについての書込制御フラグWPF、つまりU-TOCセクター0の該当トラックのトラックモードのd1ビットをオフとさせる(S103)。

【0239】このような処理により、結局、チェックアウトコンテンツについては、編集が行われない限り書込制御フラグWPFはオンである。一方、編集されたチェックアウトコンテンツ、及び編集の有無に関わらず自己録音コンテンツについては、書込制御フラグWPFはオフの状態になる。従って、図28のチェックインセッションにおけるステップF151として、チェックイン対象のコンテンツIDをパーソナルコンピュータ1から要求された際、記録再生装置20AではステップF251のチェックイン可否チェックとしては、単に、当該対象とされたコンテンツデータについての、U-TOCセクター0のトラックモードの書込制御フラグWPF(d1ビット)がオンであるか否かを確認すればよいものである。

【0240】もしコンテンツIDを要求されたコンテンツデータについて書込制御フラグWPFがオフであれば、記録再生装置20Aはパーソナルコンピュータ1に対してチェックイン不可を通知すればよい。この場合は、図28のステップF253、F152としての処理によりコンテンツIDを通知/照合して、結局チェックイン不可となることという無駄な処理が解消できる。即ち、この図28のステップF253、F152の処理は、あくまで編集されていないチェックアウトコンテンツと確認されたものについて、コンテンツID照合を行う処理となり、無駄がなくなる。このためチェックイン通信セッション及び確認処理が効率化できる。

【0241】ところで、自己録音コンテンツについては編集は基本的にフリーである。しかしながら、ミニディスク100においてチェックアウトコンテンツと自己録

音コンテンツが混在しているような場合などは、自己録音コンテンツについても自由な編集を制限したい場合がある。例えばミニディスク100におけるコンテンツデータをパーソナルコンピュータ1のアプリケーションにより管理したい場合などである。このため本例では、図24、図25に示したイクスクルーシブログインコントロールコマンド、イクスクルーシブログアウトコントロールコマンドが用意され、パーソナルコンピュータ1側から記録再生装置20Aの機能を排他制御できるようにしている。

【0242】パーソナルコンピュータ1から図24のイクスクルーシブログインコントロールコマンドが記録再生装置20Aに送信されると、システム制御部32は、そのプライオリティの値に応じて、編集禁止/制限のモードに入る。例えば図34に示すように、自己録音コンテンツについても編集その他の処理の禁止又は制限が課された状態となり(S107)、ユーザー操作による編集指示は受け付けられないものとする。なお、パワーオンやディスクジェクトなどの操作も含めて、ユーザー操作についてどのレベルまで受け付けないかは、イクスクルーシブログインコントロールコマンドにおけるプライオリティの値による、上述した制御レベルに応じて設定されるものとなる。

【0243】また、イクスクルーシブログアウトコントロールコマンドが送信された場合は、それまでの編集禁止/制限は解除され、自己録音コンテンツについては編集可能となる(S107→S106)。

【0244】このようなイクスクルーシブログインコントロールコマンドにより、パーソナルコンピュータ1側が記録再生装置20A側の機能を排他制御できることで、システム動作の都合に応じて、編集等を制限できるため、システム動作上、便利なものとなる。

【0245】14. 課金情報処理

続いて、課金情報処理について説明する。図36はコンテンツデータ配信に対する課金処理のためのシステム構成を示している。なお、このシステム構成は図4と同様であるが、コンテンツサーバ91側の構成を詳しく示したものである。

【0246】上述してきたように本例のシステムは、コンテンツとしての楽曲データ等をサーバ91側から一次記録媒体(HDD5)にダウンロードし、さらに二次記録媒体(ミニディスク100)にチェックアウトできるシステムである。もちろんコンテンツサーバ91が、コンテンツデータを有料で提供することが考えられる。

【0247】この場合コンテンツサーバ91は、コンテンツ提供サービスを行う組織や個人によって運営されるもので、基本的には、各種コンテンツを蓄積するコンテンツ保有機能、ネットワーク110を介した通信によりパーソナルコンピュータ1に対して保有しているコンテンツを提供する機能、コンテンツ提供を受けるユーザに

対する課金管理を行う課金機能、を有するものとなる。これらの各機能は、1つの組織、会社等によって全体的に運営されてもよいが、それぞれが異なる組織、会社、個人等によって運営され、連係的に動作されるものであってもよい。例えば各機能のそれぞれがインターネット上のウェブサイトとして運営され、互いにリンクにより連係動作がとられるようにしてもよい。

【0248】ユーザーサイドで最終的にコンテンツデータが記録される二次記録媒体としては、ミニディスク100やメモリカードとして述べてきたが、この二次記録媒体としてのメディアには、後述するプリペイド情報が書換不能に記録されている。コンテンツサーバ91側は、二次記録媒体に記録されているプリペイド情報を受け取ることで、個々のユーザに対する課金処理を行うものとなる。

【0249】コンテンツサーバ91は、ネットワーク配信装置130、コンテンツデータベース制御装置140、顧客情報装置150、コンテンツデータベース160、顧客データベース170を有して構成される。ネットワーク配信装置130は、ネットワーク110を介してパーソナルコンピュータ1等に、保有しているコンテンツを提供する機能を実現する部位である。コンテンツデータベース制御装置140及びコンテンツデータベース160は、各種コンテンツを蓄積するコンテンツ保有機能を実現する部位である。顧客情報装置150及び顧客データベース170は、コンテンツ提供を受けるユーザに対する課金管理を行う課金機能を実現する部位である。

【0250】コンテンツデータベース160は例えばハードディスク、光ディスクなどの記録媒体により形成され、このコンテンツデータベース160には、例えば多数の音楽コンテンツが、ユーザーに対する提供サービス用のコンテンツとして音楽ライブラリ形式で格納されている。コンテンツデータベース制御装置140は、コンテンツデータベース160に対して音楽コンテンツ等の記録、読出を制御する。例えばネットワーク配信装置130からの要求に応じてコンテンツデータベース160からコンテンツを読出、ネットワーク配信装置130に提供する。

【0251】顧客データベース170は、例えばハードディスク、光ディスクなどの記録媒体により形成され、この顧客データベース170には、個々の二次記録媒体100に記録されているプリペイド情報に対応して、課金情報が登録されている。顧客情報装置150は、顧客データベース170に対して課金情報の登録や読出の制御を行う。例えばネットワーク配信装置130からの要求に応じて、新規に課金情報を顧客データベース170に登録したり、或いは特定の課金情報を読み出してネットワーク配信装置130に提供する。

【0252】これらコンテンツサーバ91としての各部

位は、上述したように1つの組織、会社、個人等により運営されてもよいし、それぞれ異なる組織等によって運営されてもよい。例えばネットワーク配信装置130は配信サービス会社によって運営され、コンテンツデータベース制御装置140及びコンテンツデータベース160はレコード会社、レコードレーベル会社等によって運営され、顧客情報装置150及び顧客データベース170は課金サービス会社によって運営されるという形態もあり得る。また、例えばコンテンツデータベース制御装置140及びコンテンツデータベース160は複数存在し、ネットワーク配信装置130がそれぞれのコンテンツデータベース160に格納されているコンテンツを配信できるような形態もあり得る。

【0253】このような本例のシステムでは、パーソナルコンピュータ1はコンテンツサーバ91との間で通信接続を行い、提供可能なコンテンツのリスト（メニュー）を受け取る。ユーザーはリストの中で所望のコンテンツを選択する操作を行う。するとコンテンツサーバ91側からそのコンテンツがパーソナルコンピュータ1に送信されてくる。ユーザーサイドではそのコンテンツを上述してきたチェックアウトにより二次記録媒体100に記録する。これによってユーザーは所望の楽曲等を入手できるものとなる。そして本例では、コンテンツの対価の課金に関しては、二次記録媒体100に記録されているプリペイド情報を利用する。後述するが、二次記録媒体100にはプリペイド情報として個々のメディア毎に異なるメディアIDとプリペイド金額が含まれている。パーソナルコンピュータ1は記録再生装置20A（20B）からプリペイド情報を受け取って、そのプリペイド情報をコンテンツサーバ91側に送信する。ネットワーク配信装置130はそのプリペイド情報に基づいて顧客データベース170上で課金処理を実行させる。大まかにいえば、顧客データベース170には各二次記録媒体100のプリペイド情報に対応して課金情報が登録されており、コンテンツ配信に応じてその対価額を課金情報におけるプリペイド金額から減算していく。つまり課金は顧客データベース170上での課金情報の更新により行われる。そして二次記録媒体100側に記録されているプリペイド情報については、一切書換は行われないものである。

【0254】顧客データベース170には、図37のような課金情報が登録される。ここでいう課金情報とは、1つのプリペイド情報（1つの二次記録媒体100）に対応して登録されるデータ群をいい、例えばメディアID、残り金額、購入履歴などのデータから1つの課金情報が構成される。図37にはメディアIDとしてのID1～ID5・・・のそれぞれに対応して課金情報K1～K5・・・が登録されている様子を例示している。

【0255】課金情報におけるメディアIDとは、後述するプリペイド情報に含まれているメディアIDであ

る。残り金額とは、プリペイド元金からコンテンツ購入毎にその代金が引かれていくように更新されることで、現在でのプリペイド残金を示す情報である。購入履歴とは、購入日時、コンテンツ名、コンテンツ金額、使用端末などの履歴であり、つまりコンテンツ購入毎にその状況を記録した情報となる。なお、もちろんこれら以外の情報としてプリペイド元金や、メディア種別、メディア販売者、購入コンテンツの著作権者などの多様な情報が課金情報に含まれてもよいし、また例えば購入履歴は含まなくてもよい。本例の配信動作に関していえば、少なくともメディアIDと残り金額の情報が課金情報として含まれていればよく、他の情報は配信システムの運営上の都合やサービス内容などに応じて設定すればよい。

【0256】プリペイド情報は、二次記録媒体100において書換不能に記録されている情報であり、基本的に図38に示すようにプリペイド金額、プリペイドサービスID、メディアIDから構成される。プリペイド金額とは、ユーザーが先払いとして支払った金額が記録される。二次記録媒体100は、例えばコンテンツとしては何も記録されていない未使用のミニディスクやメモリーカードとして販売されるが、その販売価格はプリペイド金額を含むものとされる。つまり、未使用の場合の通常の販売価格が500円のメディアであるとしたときに、プリペイド情報においてプリペイド金額が5000円と記録されている二次記録媒体100の場合は、基本的には5500円でユーザーが購入するものとなる。もちろん販売価格は任意であり、上記二次記録媒体100が、メディア自体は無料とされてプリペイド金額のみの5000円で販売されたり、或いは4800円にディスカウントされて販売されてもかまわないが、プリペイド金額が5000円と記録された二次記録媒体100を購入したユーザーは、本例の配信システムによるコンテンツ配信サービスに関して、5000円を先払いしたこととなる。

【0257】プリペイドサービスIDは、コンテンツ配信サービスを行うコンテンツサーバ91のアドレスを表す。例えばネットワーク110においてネットワーク配信装置130に通信接続するためのアドレスである。インターネットにおけるIPアドレスであってもよい。パーソナルコンピュータ1は、記録再生装置20Aに装填された二次記録媒体100についてのプリペイド情報を受け取ることで、プリペイドサービスIDに基づいて、コンテンツサーバ91に通信アクセスを行い、接続を求めることができる。なおコンテンツサーバ91側の構成にもよるが、プリペイドサービスIDは、ネットワーク配信装置130のアドレスではなく、例えばコンテンツデータベース制御装置140のアドレスとしたり、或いは顧客情報装置150のアドレスとしてもよい。例えばネットワーク配信装置130、コンテンツデータベース制御装置140、顧客情報装置150がそれぞれインタ

ーネット上のWebページとして形成され、互いにリンクされるような場合、プリペイドサービスIDをコンテンツデータベース制御装置140のアドレスとして、パーソナルコンピュータ1はコンテンツデータベース制御装置140に対して通信アクセスを行うようにし、その際に、配信処理の進行に応じて顧客情報装置150がリンクされ、さらにこれらがネットワーク配信装置130によって統括処理されるようにすることも考えられる。逆にプリペイドサービスIDを顧客情報装置150のアドレスとして、パーソナルコンピュータ1は顧客情報装置150に対して通信アクセスを行うようにし、その際に、配信処理の進行に応じてコンテンツデータベース制御装置140がリンクされ、さらにこれらがネットワーク配信装置130によって統括処理されるようにすることも考えられる。

【0258】メディアIDは、個々の二次記録媒体100についてそれぞれ固有に付された識別ナンバである。例えばユーザーが2枚のプリペイドメディアとしての二次記録媒体100を購入した場合、その各二次記録媒体100には、それぞれ異なるメディアIDが記録されていることになる。

【0259】このようなプリペイド情報は、例えばプリペイド金額に8ビット、プリペイドサービスIDに22ビット～32ビット程度、メディアIDに32～40ビット程度を用いたデータとすることができる。ビット数はプリペイドシステムの設計上の都合で決められればよい。またプリペイドサービスIDには、サーバのアドレス等のために必要なビット数、メディアIDには、販売するプリペイドメディアの総数や将来的な総数などを勘案して、個々に異なるIDナンバを降ることができるために十分なビット数とされればよい。最低限としては、例えばプリペイド金額に1バイト(8ビット)、プリペイドサービスIDに3バイト又は4バイト、メディアIDに3バイト又は4バイトとして、8バイト程度のデータとされればよい。

【0260】ここで、二次記録媒体100に記録されるプリペイド情報と、図37に示した課金情報の関係について述べておく。例えばメディアID=ID1、プリペイド金額=5000円とされた二次記録媒体100をユーザーが使用したとする。コンテンツサーバ91側では、この二次記録媒体100が最初に使用された時点で、顧客データベース170に、図37の課金情報K1を登録する。当初、この課金情報K1におけるメディアID及び残り金額は、プリペイド情報上のデータがそのまま登録されることになり、つまり課金情報K1のメディアID=ID1とされ、残り金額=5000円とされる。その後、その二次記録媒体100を使用してコンテンツのダウンロード(二次記録媒体100へのチェックアウト)が行われることに応じて、そのコンテンツの代価が、課金情報K1の残り金額の減額という形で課金処

理されることになる。つまり、ダウンロード/チェックアウトが行われる毎に、使用されている二次記録媒体100のプリペイド情報におけるメディアIDから、顧客データベース170上で対応する課金情報が検索され、その課金情報上で残り金額の減算が行われる。例えば図37の課金情報K1では残り金額が3700円とされているが、これはユーザーがメディアID=ID1の二次記録媒体100を用いて、1300円分のコンテンツ購入を行った後の状態として示されているものとなる。

【0261】そしてこのような課金処理方式からわかるように、ユーザーが所有する二次記録媒体100においてはプリペイド情報は全く更新されないものとなり、換言すれば、プリペイド情報は二次記録媒体100において書換不能に記録されていけばよいものとなる。なお、プリペイド情報は二次記録媒体100において書換可能としてもよいが、プリペイド金額やメディアIDの改竄による悪用や、プリペイドサービスIDの改竄によるサービス動作の不具合のおそれもあるため、書換不能とすることが適切である。

【0262】上述のように二次記録媒体100としてミニディスクを使用する場合において、8バイトのプリペイド情報を書換不能に記録しておく記録方式は次のような各例が考えられる。

- (1) P-TOC内にプリペイド情報を記録する
- (2) U-TOC内に書換不能となる手法でプリペイド情報を記録する。
- (3) 管理エリア内でU-TOC領域外に書換不能となる手法でプリペイド情報を記録する。

【0263】P-TOC内にプリペイド情報を記録する場合は、例えば図9(a)のリードインエリアにおけるP-TOCセクターにおいて特定の8バイトの領域を、プリペイド情報の記録に用いることが考えられる。

【0264】U-TOC内に記録する場合は、例えば既にフォーマットが規定されているセクター0, 1, 2, 3, 4などにおける未使用の領域を利用してもよいが、プリペイド情報が書換えられる可能性を適切に排除するには、まだ規定されていないセクターを利用することが考えられる。例えばU-TOCセクター5において所定の8バイトをプリペイド情報の記録領域として設定するものである。そしてさらにこの場合は、上述したU-TOCセクター0において、セクター使用状況(Used sectors)におけるセクター5の対応ビットを「0」、つまり使用していないセクターとして表されるようにすることで、プリペイド情報を書換不能とできる。つまりこれにより一般のミニディスクレコードによれば、U-TOCセクター5は使用されていないセクターとして認識されるため、U-TOCセクター5について何らかの更新処理等が行われることはない。つまりプリペイド情報はユーザーサイドで書換不能とされる。そして本例の記録再生装置20Aでは、プリペイド情報の読出のためのアプ

リケーションプログラムに基づいて、U-TOCセクタ5の読込を実行するものとされていることにより、プリペイド情報を読み出すことができる。なお、ここではセクタ5としたが、もちろんセクタ6、セクタ7など他のセクタを利用してもよい。

【0265】また図9(b)の管理エリア内であって、U-TOC以外の領域に記録する方式として、例えば斜線部PDとして示すように、使用されていないクラスタ内のセクタを利用してプリペイド情報を記録することが考えられる。管理エリア内ではパワーキャリブレーションエリアPCAやU-TOCエリアが形成され、これらの位置は上述したようにP-TOCによって示されるものとなる。P-TOCを参照することによって通常のミニディスクレコーダはパワーキャリブレーションエリアPCAやU-TOCエリアにアクセスできる。ところがP-TOCによって位置が示されていない斜線部PDは、通常のミニディスクレコーダではアクセスできない領域（アクセスしても意味のない領域）となる。従って、斜線部PDに記録されたプリペイド情報はユーザーサイドで書換不能とされる。そして本例の配信システムに用いる記録再生装置20Aでは、プリペイド情報の読出のためのアプリケーションプログラムに基づいて、斜線部PDの読込を実行するものとされていることにより、プリペイド情報を読み出すことができる。このためには例えば、斜線部PDの開始位置を、P-TOCに示されるU-TOCスタートアドレスに所定量のオフセットを与えた位置と規定しておくことで、記録装置10によってプリペイド情報の読出が可能となる。例えばU-TOCは3クラスタにわたって記録されるため、U-TOCスタートアドレスUSTA+5クラスタの位置をプリペイド情報記録領域の開始位置と規定すればよい。

【0266】例えば以上の例のようにすることで、ミニディスクをプリペイドメディア4として用いることができる。またミニディスクについて説明したが、二次記録媒体100としてメモ리카ードや、CD-R、CD-RW、DVD等の光ディスクの場合についても、8バイト或いはそれ以上のデータサイズのプリペイド情報を記録する場合は、それらのメディアの管理フォーマット等に基づいて、記録位置が設定されればよい。

【0267】ところで、このようなプリペイド情報を用いた配信システムを構築する場合、パーソナルコンピュータ1は記録再生装置20Aに装填された二次記録媒体（ミニディスク100）についてのプリペイド情報を読み出せるようにする必要がある。このため、図20、図21で説明したようにチェックインコントロールコマンドにおいてサブファンクションでプリペイド情報を指定することで、記録再生装置20Aにプリペイド情報を要求できるようにしている。また記録再生装置20Aは、図23のチェックインレスポンスコマンドによって、ミニディスク100に記録されているプリペイド情報をパ

ーソナルコンピュータ1に通知できる。

【0268】図35は、プリペイド情報処理のための処理を示している。図35において、パーソナルコンピュータ1のCPU2が実行する制御処理をステップF101～F173とし、また記録再生装置20Aのシステム制御部32、MD制御部21等によって実行される制御処理をステップF201～F274として示している。通信セッションは各種のコントロールコマンドとそれに対応するレスポンスコマンドにより行われる。

【0269】この場合も、認証開始からEKB転送、ルートキー探索等の処理は上記チェックアウトの場合と同様に行われる。即ち上記図26、図28と同一のステップ番号を付したステップF101～F103、F201～F205は、上述と同様の処理が行われるものであり、重複説明を避ける。

【0270】パーソナルコンピュータ1はステップF170で、セッションの開始を要求するコントロールコマンドを送信する。これに応じて記録再生装置20AはステップF270で、レスポンスコマンドを返す。なお、この場合にも、図12で説明した認証処理が行われる。

【0271】セッションが開始され、且つ記録再生装置20Aが認証OKとなったら、パーソナルコンピュータ1はステップF171として、プリペイド情報を要求する。つまり、図20で説明したチェックインコントロールコマンドを送信するものとなる。このときチェックインコントロールコマンドにおいては、サブファンクションの値は「00h」又は「01h」ではなく、つまりプリペイド情報要求の意味を持たせたものとする（図21参照）。

【0272】記録再生装置20Aは、これに応じてステップF271で、上述のようにミニディスク100の特定の領域に記録されているプリペイド情報を再生する。そしてステップF272で、再生した例えば8バイトのプリペイド情報を、図23のようにチェックインレスポンスコマンドにセットして、パーソナルコンピュータ1に送信する。

【0273】チェックインレスポンスコマンドによりプリペイド情報を受け取ったら、パーソナルコンピュータ1はステップF172でセッション終了要求のコントロールコマンドを記録再生装置20Aに送信する。記録再生装置20AはステップF273としてセッション終了を了承するレスポンスコマンドをパーソナルコンピュータ1に送信する。またパーソナルコンピュータ1はステップF173で、認証状態を終了させるコントロールコマンドを送信し、記録再生装置20AはステップF274で、認証状態終了を了承するレスポンスコマンドを送信する。以上で、プリペイド情報受け渡しのための通信が終了される。

【0274】その後、パーソナルコンピュータ1はプリペイド情報に対する処理として、通信部8によりネット

ワーク 110 を介してコンテンツサーバ 91 と通信接続し、受け取ったプリペイド情報を、コンテンツサーバ 91 に転送する処理を行う。即ち、二次記録媒体 100 に対してチェックアウトしたコンテンツデータの識別情報とともにプリペイド情報を送信することで、コンテンツサーバ 91 側でユーザーに対する課金処理、即ち図 37 のデータベースの更新処理が行われるようにするものである。

【0275】このようにパーソナルコンピュータ 1 が記録再生装置 20A に対して二次記録媒体 100 における固有情報であるプリペイド情報の転送を要求でき、当該システムによるプリペイド方式の課金処理が可能となる。

【0276】なお、本例としてパーソナルコンピュータ 1 が二次記録媒体 100 の固有情報としてプリペイド情報を取得する方式を述べたが、同様のコントロールコマンド及びレスポンスコマンドの設定によって、各種の固有情報取得が可能となることはいうまでもない。例えば二次記録媒体 100 に記録されたユーザーの利用状況、ユーザー ID など、他の固有情報をパーソナルコンピュータ 1 が取得することで、パーソナルコンピュータ 1 が二次記録媒体 100 の管理を行ったり、或いはそれらの情報をコンテンツサーバ 91 に送信して、コンテンツサーバ 91 側がユーザーに対する各種サービスや管理に用いることが想定できる。

【0277】以上、実施の形態としての例を説明してきたが、本発明は上記例に限定されるものではない。システム動作としての暗号化、データベース、チェックアウト／チェックイン方式、認証方式、コンテンツ ID 生成方式、コンテンツ ID 管理方式、書込制御フラグの実際の例、編集管理、プリペイド情報などは、それぞれ発明の要旨の範囲内で各種変形例が考えられる。

【0278】また本発明としては、例えば上述してきた一次記録媒体から二次記録媒体へのデータ転送処理の対象となるのは SDMI コンテンツに限らず、各種のコンテンツデータに広く適用できる。また一次記録媒体は HDD 以外に多様に考えられる。もちろん二次記録媒体、二次記録媒体側機器 20A としてもミニディスク、ミニディスク記録装置に限らず、多様な例が考えられる。二次記録媒体 100 としては、CD-R、CD-RW、DVD-RAM、DVD-R、DVD-RW、各種メモリカードなどであってもよい。従って二次記録媒体側機器 20A は、これらのメディアに対応する記録装置であればよい。また、SDMI 対応の記録再生装置 20B についても言及したが、その記録再生装置 20B へのコンテンツデータの転送処理においても本発明は適用できる。

【0279】

【発明の効果】以上の説明からわかるように本発明によれば、データ転送装置側（一次記録媒体側）では、格納

されている各コンテンツデータについての転送権利を管理するとともに、データ記録装置（二次記録媒体側）に対して転送したコンテンツデータについては、そのコンテンツデータに対応する第 1 のコンテンツ識別子とデータ記録装置側から送信されてきた第 2 のコンテンツ識別子を対応させたテーブルデータを生成した状態で、コンテンツデータの転送権利を管理するようにしている。つまり、二次記録媒体側でコンテンツ識別子（コンテンツ ID）を記録できない場合でも、二次記録媒体側で発生させるコンテンツ ID（第 2 のコンテンツ識別子）を用いて二次記録媒体上のコンテンツデータを識別でき、しかもそれが一次記録媒体側のコンテンツ ID（第 1 のコンテンツ識別子）と対応づけられているため、コンテンツ ID による適切なチェックアウト／チェックイン時の権利管理が可能となる。従って非 SDMI 対応の二次記録媒体においてコンテンツデータを非暗号化状態で記録する場合にも、コピー転送や再生に関してのコンテンツ権利が適切に管理でき、ユーザーの利便性と著作権保護を両立できる。

【0280】また、二次記録媒体に対する記録再生を行うデータ記録装置側での第 2 のコンテンツ識別子の生成に関しては、非暗号化状態のコンテンツデータの一部を抽出した演算で第 2 のコンテンツ識別子を生成することで、各コンテンツデータ毎に固有のコンテンツ ID として生成できる。また、コンテンツデータのデータ長に基づいて特定されたサンプリングポイントによりコンテンツ ID 生成に用いるコンテンツデータの一部を抽出するというように、抽出ポイントが設定されていることで、各コンテンツデータについては、常にそれぞれ特定のコンテンツ ID を生成できる。つまり第 2 のコンテンツ識別子自体を記録しておかなくても、二次記録媒体側のコンテンツデータから特定の第 2 のコンテンツ識別子を常に得られるため、上記の権利管理に用いる情報として好適なものとなる。また、上記サンプリングポイントは、コンテンツデータの先頭部分及び終端部分を除いた 1 又は複数のポイントとすることで第 2 のコンテンツ識別子を、各コンテンツデータに固有の情報として適切なものとする。例えばオーディオコンテンツの場合、先頭及び終端は無音状態などであって、データ自体が他のコンテンツと同じものとなっている場合が多いが、それ以外の部分は、データ自体が他のコンテンツと同じということはまずあり得ないからである。

【0281】また、チェックアウトとしてデータ転送装置からコンテンツデータが転送されてくる際には、復号されたコンテンツデータを二次記録媒体に記録するまでのデータ経路上で、上記サンプリングポイントのデータを抽出しておき、抽出したデータを用いた演算処理により第 2 のコンテンツ識別子を生成するようにすることで、第 2 のコンテンツ識別子の算出のために、二次記録媒体に読出アクセスを行ってサンプリングポイントのデ

ータを得るという動作は不要となる。従ってチェックアウト時に、データ転送装置側に第2のコンテンツ識別子を通知する処理を効率化でき、一連のチェックアウト通信動作を高速化できる。

【0282】また、コンテンツデータが記録された二次記録媒体がデータ記録装置に装填されている場合には、チェックイン要求が無い時点で、二次記録媒体に記録されている各コンテンツデータについて、予め上記サンプリングポイントのデータを再生して記憶させておくこと、或いは更に第2のコンテンツ識別子の算出までを行って記憶させておくことで、チェックイン等のために第2のコンテンツ識別子が要求された際に、二次記録媒体のアクセスは不要である。従ってこの場合もチェックイン等のための一連の通信動作を高速化できる。

【図面の簡単な説明】

【図1】本発明の実施の形態で利用される暗号化方式のツリー構造の説明図である。

【図2】実施の形態で利用される暗号化方式のEKBの説明図である。

【図3】実施の形態で利用される暗号化方式のEKBの構造の説明図である。

【図4】実施の形態のシステム構成のブロック図である。

【図5】実施の形態のSDMIコンテンツのデータパス例の説明図である。

【図6】実施の形態の一次記録媒体側機器のブロック図である。

【図7】実施の形態の二次記録媒体側機器のブロック図である。

【図8】ミニディスクシステムのクラスタフォーマットの説明図である。

【図9】ミニディスクのエリア構造の説明図である。

【図10】ミニディスクシステムのU-TOCセクター0の説明図である。

【図11】ミニディスクシステムのU-TOCセクター0のリンク形態の説明図である。

【図12】実施の形態の認証処理のフローチャートである。

【図13】実施の形態の配信／転送されるコンテンツデータ及び暗号化状態の説明図である。

【図14】実施の形態の暗号化方式例及びDNKの説明図である。

【図15】実施の形態のコンテンツデータの暗号解除手順の説明図である。

【図16】実施の形態のチェックアウトコントロールコマンドの説明図である。

【図17】実施の形態のチェックアウトレスポンスコマンドの説明図である。

【図18】実施の形態のレコードオブジェクトコントロールコマンドの説明図である。

【図19】実施の形態のレコードオブジェクトレスポンスコマンドの説明図である。

【図20】実施の形態のチェックインコントロールコマンドの説明図である。

【図21】実施の形態のチェックインコントロールコマンドのサブファンクションの説明図である。

【図22】実施の形態のチェックインレスポンスコマンドの説明図である。

【図23】実施の形態のチェックインレスポンスコマンドの説明図である。

【図24】実施の形態のイクスクルーシブログインコントロールコマンドの説明図である。

【図25】実施の形態のイクスクルーシブログアウトコントロールコマンドの説明図である。

【図26】実施の形態のチェックアウト動作のフローチャートである。

【図27】実施の形態のチェックアウト動作のフローチャートである。

【図28】実施の形態のチェックイン動作のフローチャートである。

【図29】実施の形態のコンテンツID生成の説明図である。

【図30】実施の形態のコンテンツID対応テーブルの説明図である。

【図31】実施の形態のチェックアウト時のコンテンツID生成処理のフローチャートである。

【図32】実施の形態のチェックイン前のコンテンツID生成処理のフローチャートである。

【図33】実施の形態のチェックイン前のコンテンツID生成処理のフローチャートである。

【図34】実施の形態の書込制御フラグによる動作の説明図である。

【図35】実施の形態の課金情報読出動作のフローチャートである。

【図36】実施の形態の課金管理システムの説明図である。

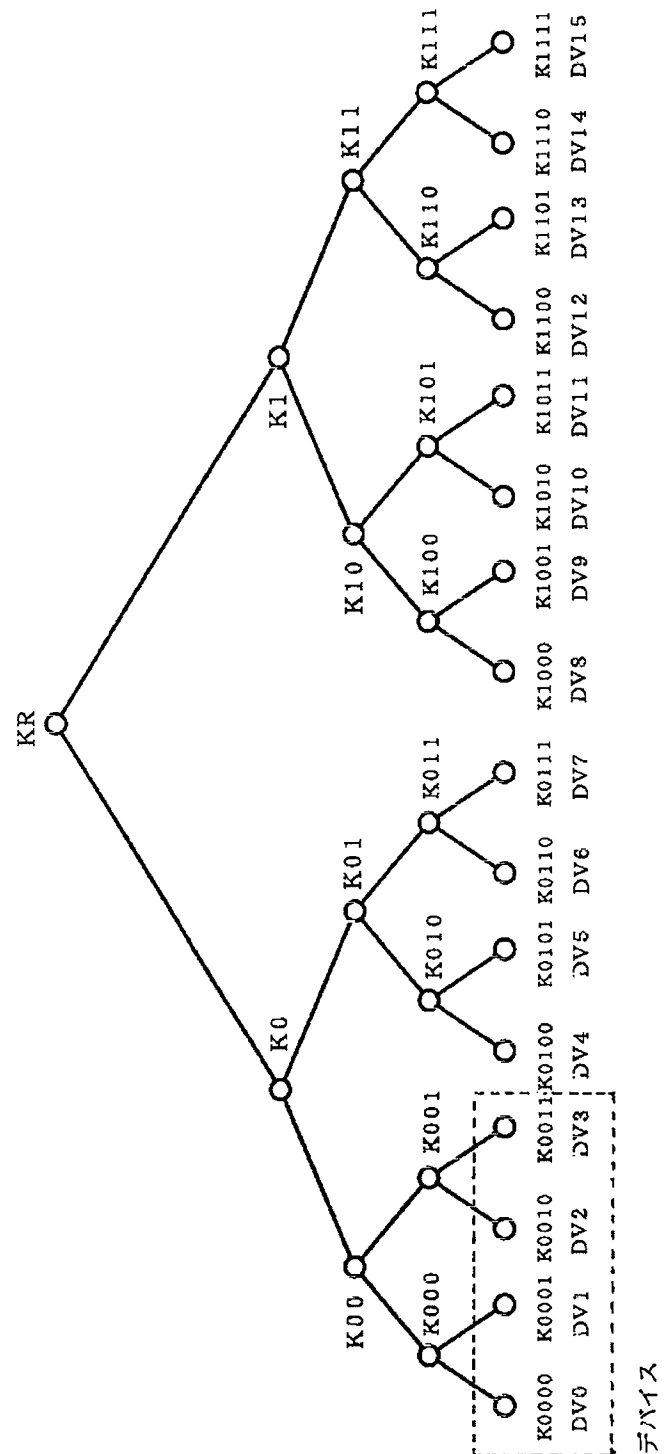
【図37】実施の形態の顧客データベースの説明図である。

【図38】実施の形態のプリペイド情報の説明図である。

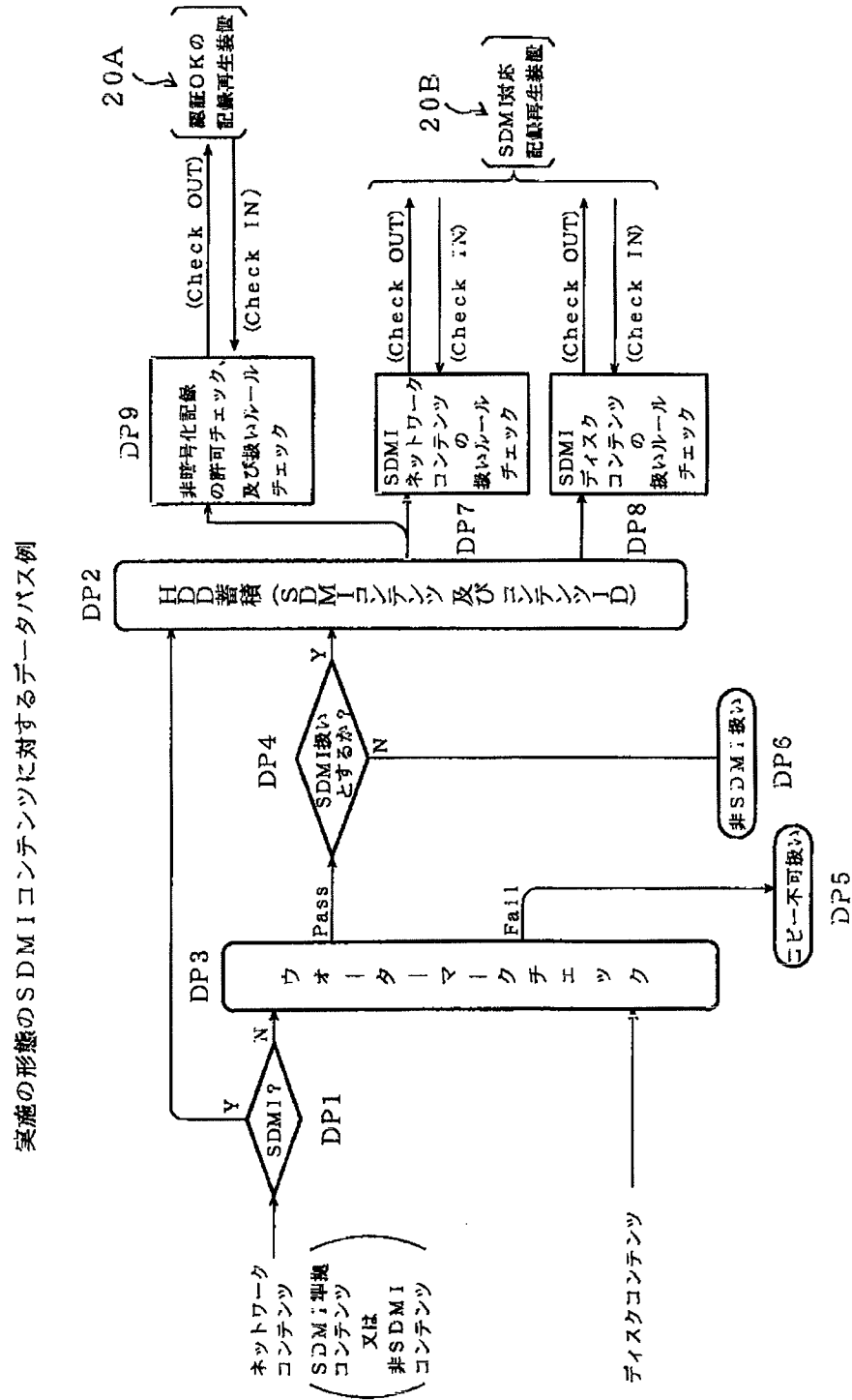
【符号の説明】

- 1 一次記録媒体側機器（パーソナルコンピュータ）、
- 2 CPU、5 HDD（一次記録媒体）、8 通信部、9 ディスクドライブ、11 接続部、20A 二次記録媒体側機器（記録再生装置）、21 MD制御部（CPU）、25記録／再生部、26 インターフェース部、28 復号部、30 バッファメモリ、31 システム制御部、100 二次記録媒体（ミニディスク）

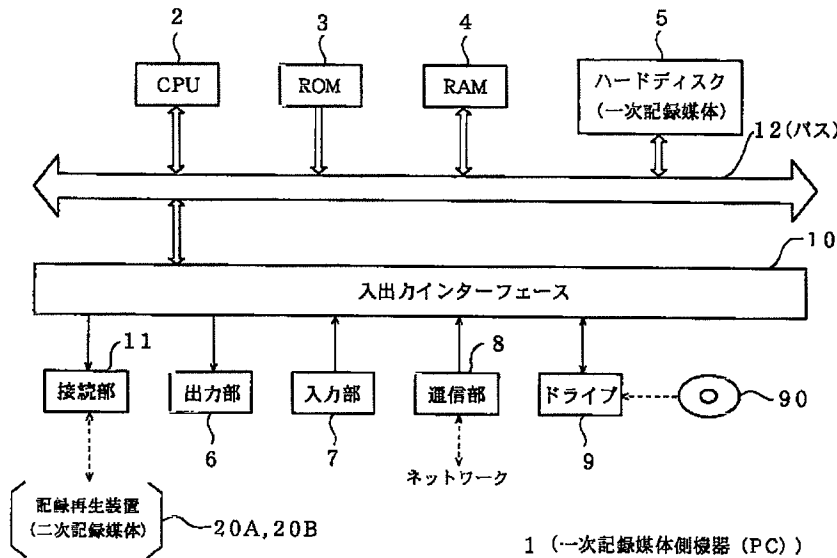
【図1】



【図5】



【図6】

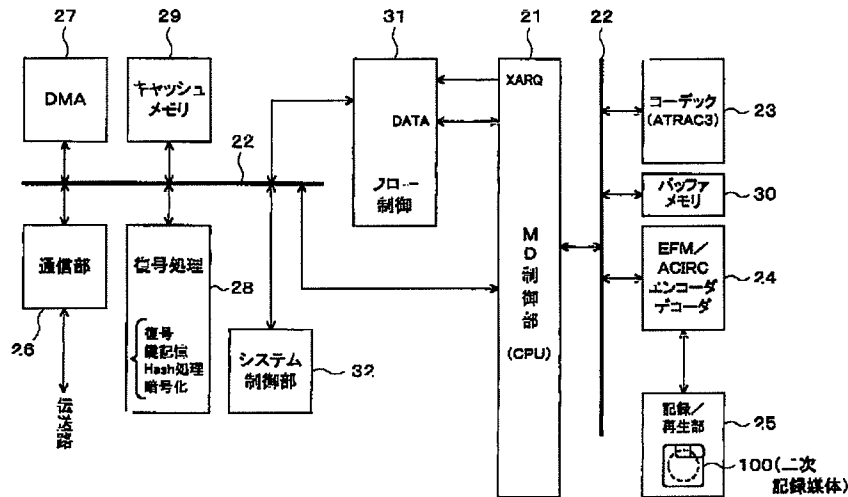


【図20】

オフセット (バイト)	MSB								LSB							
	7	6	5	4	3	2	1	0								
00h	CTS								c type : CONTROL							
...	...															
0Ah	Op Code : Check In															
0Bh	result															
0Ch	Subfunction															
0Dh																
0Eh	List ID															
0Fh																
10h	object position number															

【図7】

20A(二次記録媒体側機器(記録再生装置))



【图24】

【图25】

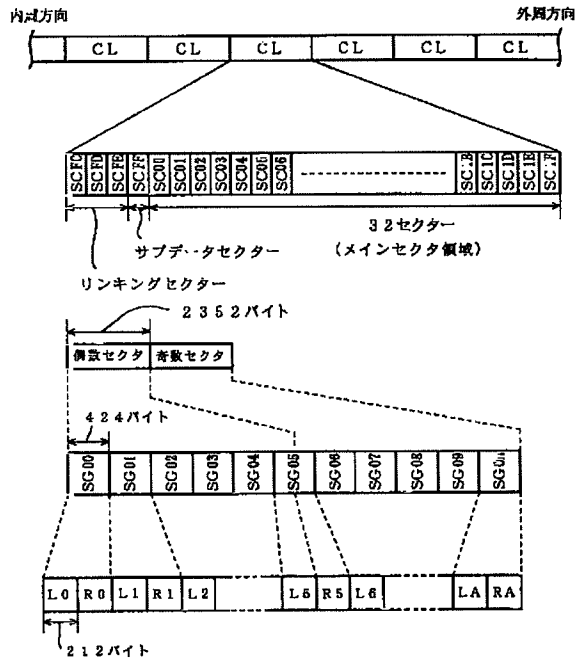
Exclusive Login Control Command

オフセット (バイト)	MSB								LSB							
	7	6	5	4	3	2	1	0								
00h	CTS								c type: CONTROL							
01h	subunit type								subunit ID							
02h	Reserved															
03h	priority															

Exclusive Logout Control Command

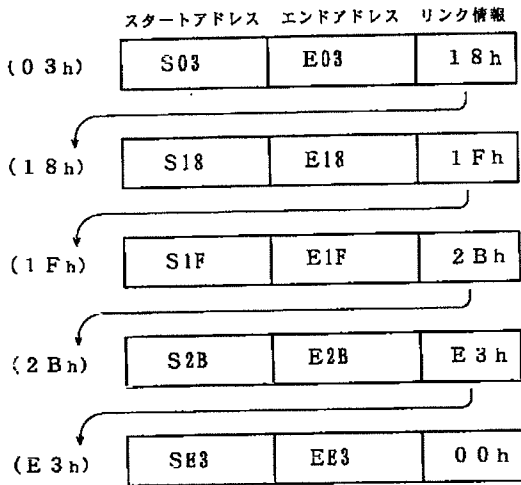
オフセット (バイト)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c type : CONTROL							
01h	subunit type								subunit ID							
02h	Reserved															
03h	priority : 00h															

【図8】

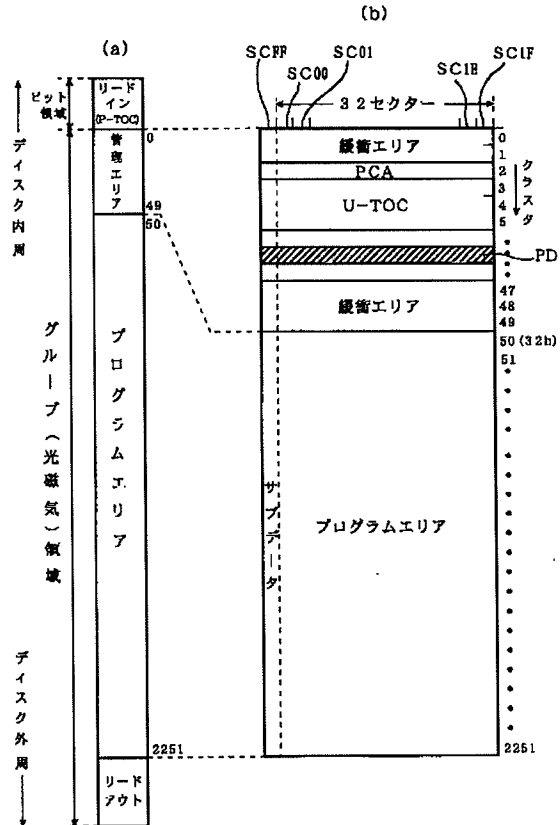


【図11】

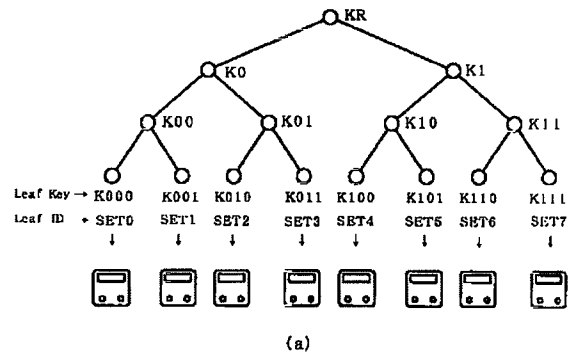
P-FRA = 03h



【図9】



【図14】



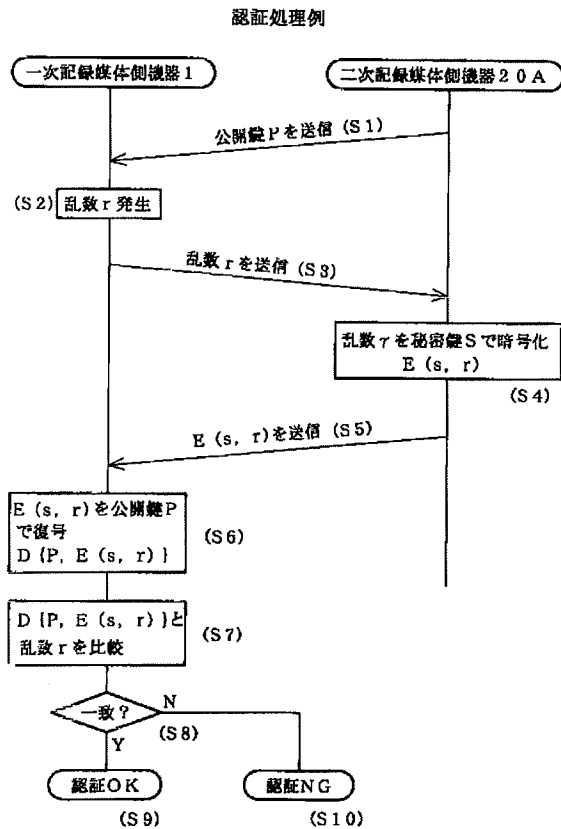
SET0のDNK (Device Node Key) 例

Leaf ID=SET0
Leaf Keyで暗号化したKR E (K000, KR)
Leaf Keyで暗号化したK0 E (K000, K0)
Leaf Keyで暗号化したK00 E (K000, K00)
Leaf Key=K000

(b)

PGアプリケーションによる コンテンツID1	二次記録媒体制御部による コンテンツID1
PGアプリケーションによる コンテンツID2	二次記録媒体制御部による コンテンツID2
PGアプリケーションによる コンテンツID3	二次記録媒体制御部による コンテンツID3

【図12】

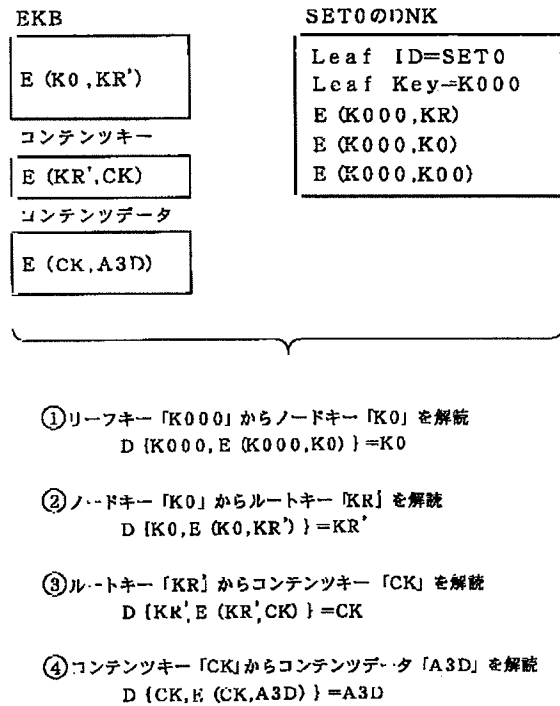


【図18】

Record Object Control Command

オフセット (バイト)	MSB	7	6	5	4	3	2	1	0	LSB
00h	CTS				c type : CONTROL					
01h	...									
0Ah	Op Code : Record Object									
0Bh	result									
0Ch	Reserved									
0Dh										
0Eh										
0Fh										
10h	Destination List ID									
11h	new object position number									
12h	content type									
13h	Download Format Track Attribute									
14h	Track Mode									
15h	Content Size									
16h										
17h										
18h										
19h	Bulk Data Size									
1Ah										
1Bh										
1Ch										
1Dh	Bulk Data Size									

【図15】

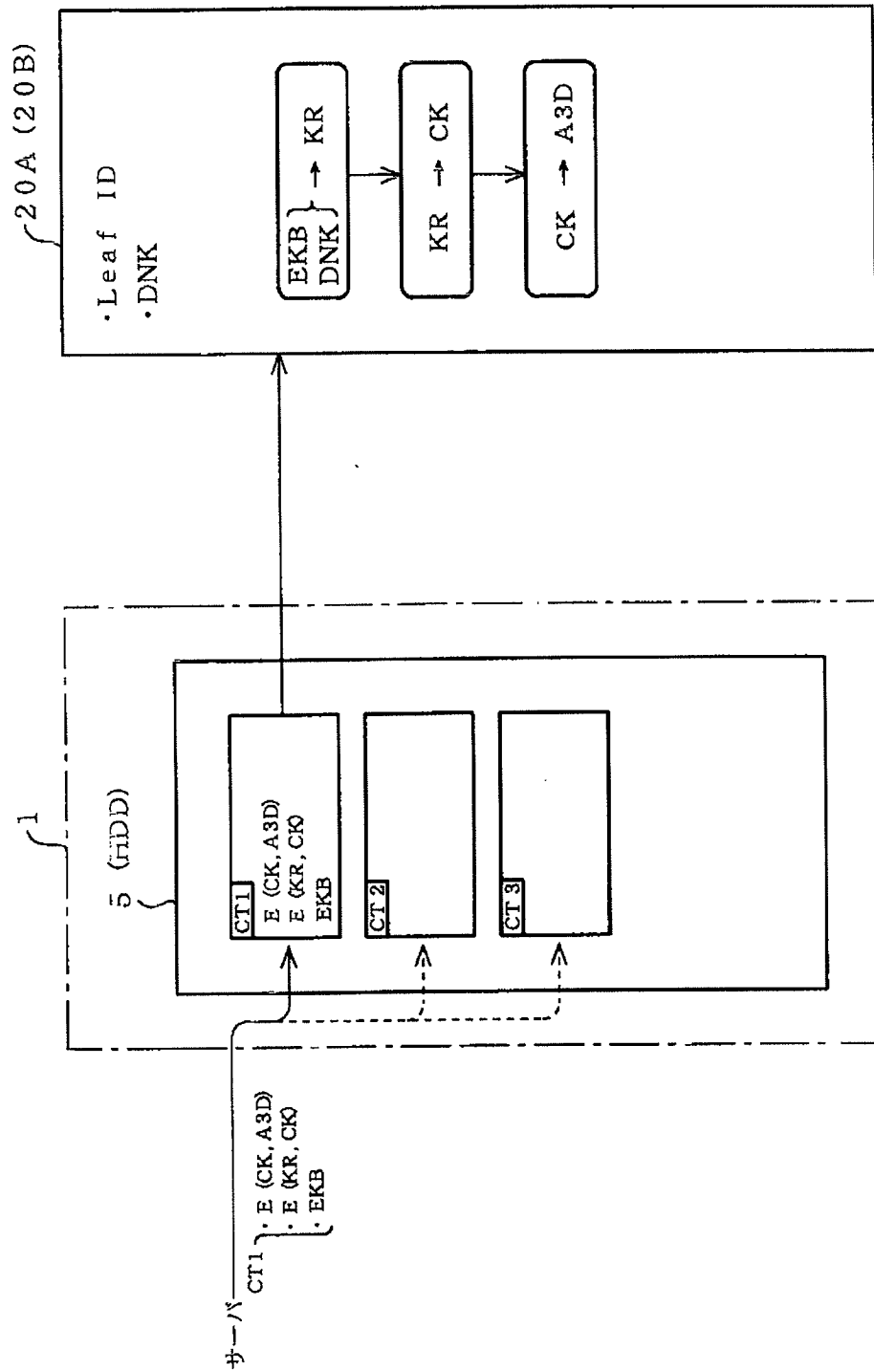


【図19】

Record Object Response Command (Accepted)

オフセット (バイト)	MSB	7	6	5	4	3	2	1	0	LSB
00h	CTS				response : ACCEPTED					
01h	...									
0Ah	Op Code : Record Object									
0Bh	result									
0Ch	Reserved									
0Dh										
0Eh										
0Fh										
10h	Destination List ID									
11h	new object position number									
12h	content type									
13h	Download Format Track Attribute									
14h	Track Mode									
15h	Content Size									
16h										
17h										
18h										
19h	Bulk Data Size									
1Ah										
1Bh										
1Ch										
1Dh	Bulk Data Size									
1Eh	Session DATA (32 byte) (コンテンツ ID)									
1Fh										
20h										
21h										

【図13】



【図22】

Check In Response Command

オフセット (バイト)	MSB					LSB				
	7	6	5	4	3	2	1	0		
00h	CTS				response : ACCEPTED					
01h					
0Ah	Op Code : Check In									
0Bh	result									
0Ch	Subfunction									
0Dh	List ID									
0Eh										
0Fh	object position number									
10h										
11h	Hash MAC (コンテンツ ID)									
12h										
13h										
14h										
15h										
16h										
17h										
18h										

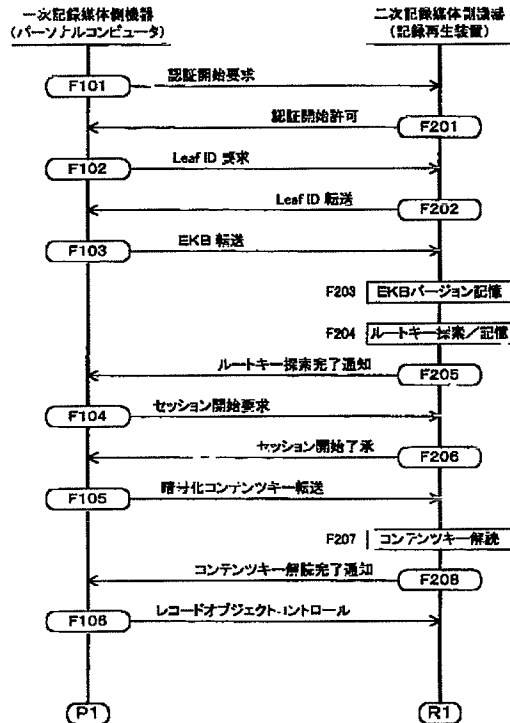
【図23】

Check In Response Command

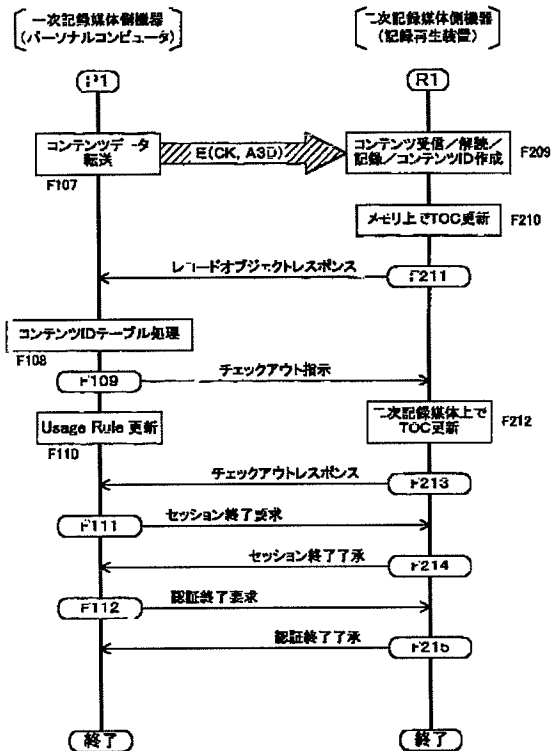
オフセット (バイト)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				response : ACCEPTED				
⋮	⋮				⋮				
0Ah	Op Code : Check In								
0Bh	result								
0Ch	Subfunction								
0Dh	List ID								
0Eh									
0Fh	object position number								
10h									
11h	プリバード情報								
12h									
13h									
14h									
15h									
16h									
17h									
18h									

【図26】

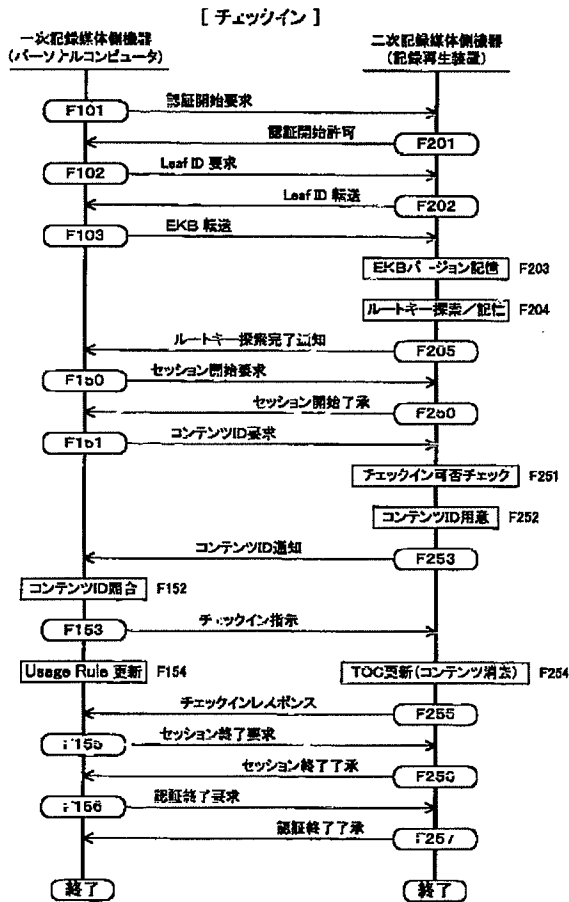
【チェックアウト】



【図27】

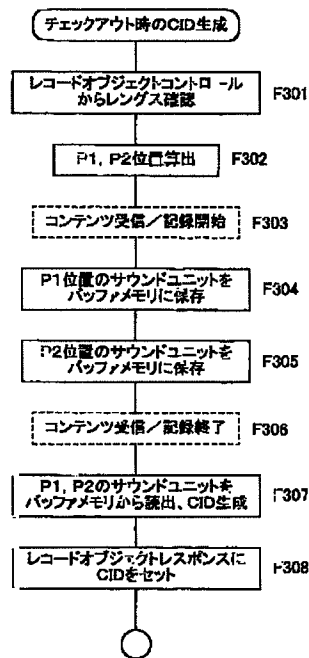


【図28】

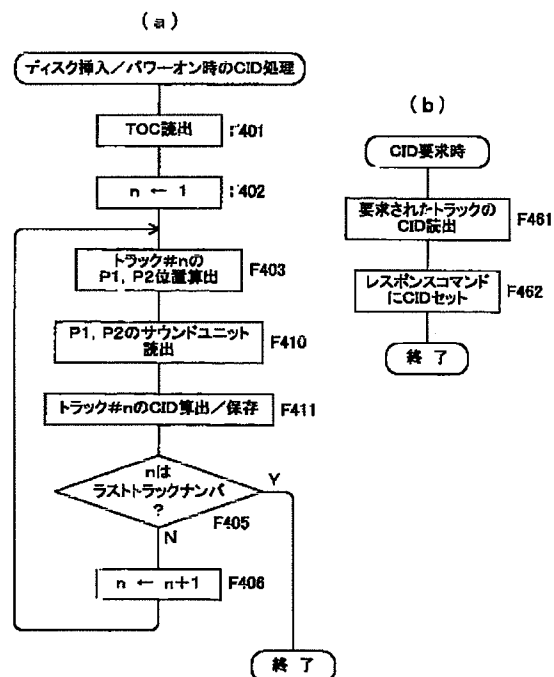
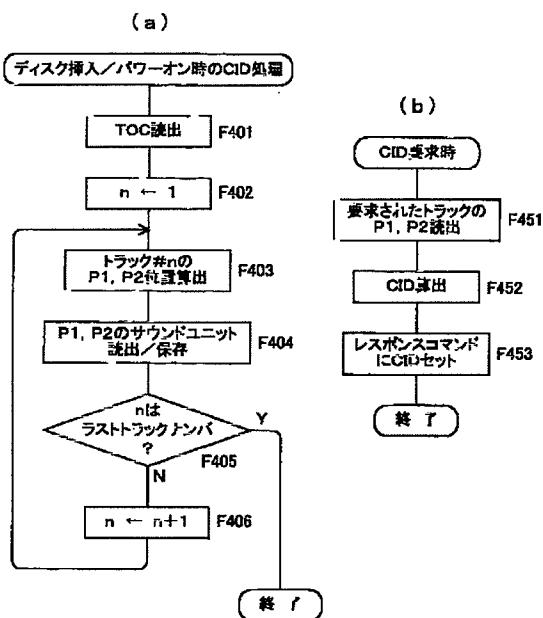


【図32】

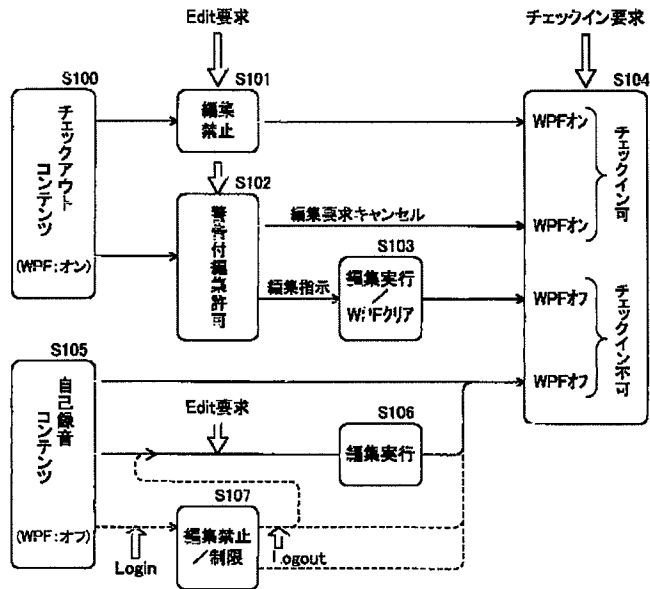
【図31】



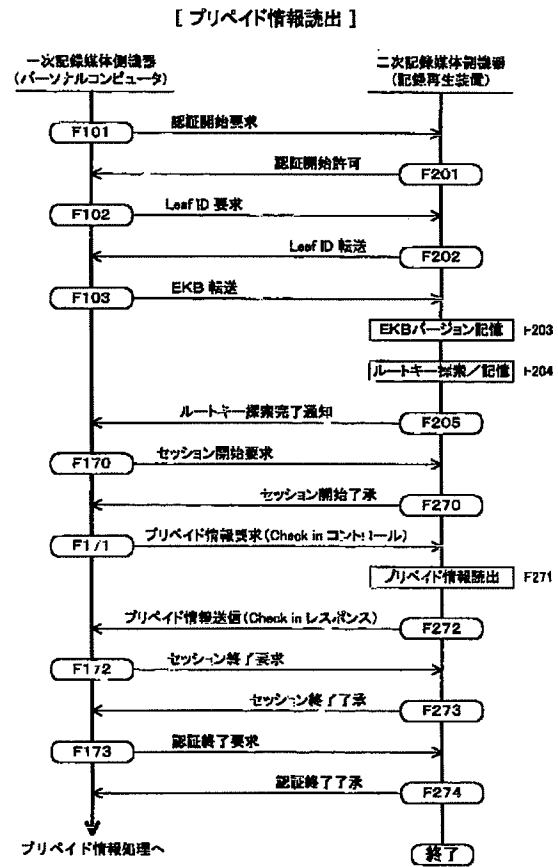
【図33】



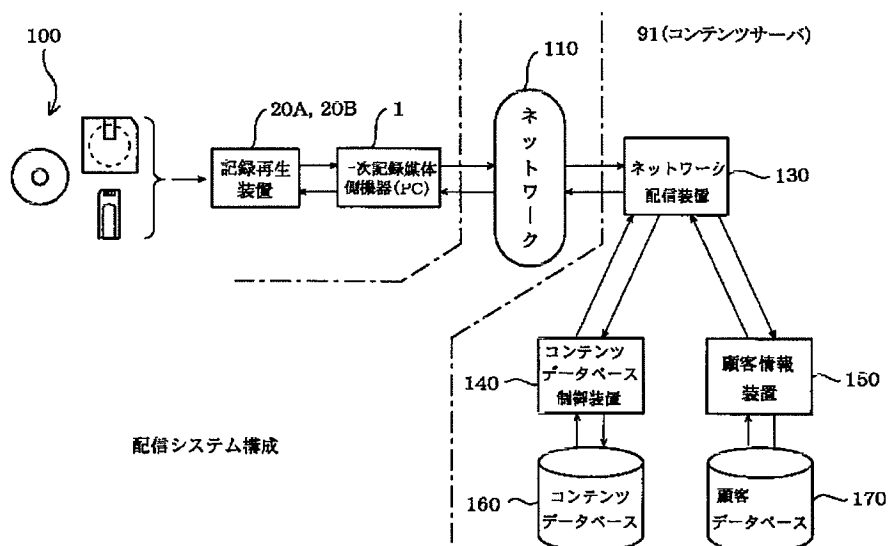
【図34】



【図35】



【図36】



【図37】

顧客データベース

	メディアID	残り金額	購入履歴
(K1)	ID1	3700円
(K2)	ID2	100円
(K3)	ID3	1200円
(K4)	ID4	5000円
(K5)	ID5	0円
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

【図38】

プリペイド情報		
プリペイド金額	プリペイドサービスID	メディアID

フロントページの続き

(51)Int.Cl.⁷ 識別記号 F I (参考)
H 0 4 N 7/173 6 3 0 H 0 4 L 9/00 6 0 1 B

(72)発明者 松田 寛美 Fターム(参考) 5B017 AA06 BA07 CA15
 東京都品川区北品川6丁目7番35号 ソニ 5B082 EA11
 ー株式会社内 5C064 BA07 BB02 BC04 BC18 BC22
(72)発明者 田中 理生 BC25 BD02 BD07 BD14
 東京都品川区北品川6丁目7番35号 ソニ 5J104 AA07 NA05 PA14
 ー株式会社内